RESEARCH ARTICLE

Administrative Responsibility for Digital Technical Failures in the Era of Government Digitization: Challenges of Digital Governance and Accountability

Hanifi Hadda
Faculty of Law and Political Sciences, University of Abderrahmane Mira - Béjaia
Russian Federation
Email: hadda.hanifi@univ-bejaia.dz

Issue web link https://imcra-az.org/archive/385-science-education-and-innovations-in-the-context-of-modern-problems-issue-11-vol-8-2025.html

Keywords Digital Government, Digitization, Administrative Responsibility, Technical Failures.

Abstract
The world is witnessing a widespread digital transformation that has led to an increasing reliance on digital technology in various fields, including public administration and government institutions. Transformation is no longer just an option, but rather a strategic necessity to enhance efficiency and transparency and achieve sustainable development goals. Digital governance represents a new management framework based on exploiting modern technology to organize administrative processes and provide public services electronically, which contributes to improving citizens' lives and increasing their satisfaction with government performance. Our current study aims to shed light on government digitization, its most important principles, the digital technical failures that can occur, and their main causes, concluding with an examination of the administration's responsibility for these digital technical failures.

Citation. Hadda H. (2025). Administrative Responsibility for Digital Technical Failures in the Era of Government Digitization: Challenges of Digital Governance and Accountability. *Science, Education and Innovations in the Context of Modern Problems*, 8(11), 182–209. https://doi.org/10.56352/sei/8.11.14

Received: 12.02.2025 | Accepted: 01.07.2025 | Published: 28.08.2025 (available online)

Introduction:

In the sphere of administration, digitalization has become a pressing need, particularly when it comes to administering public facilities or services. This has been linked to the idea of e-management and e-government, in which citizens get public services via digital platforms and channels. Therefore, when compared to traditional administration, electronic administration marked a significant turning point in terms of the efficient, quick, and transparent services it offers to individuals. However, there may be hazards associated with the digital transformation of government-provided public infrastructure and services that result in harm to citizens for which the state is liable. Stated differently, the administrative obligation incurred in cases of significant and non-serious service errors/flaws is not eliminated by the digitization of public services. Therefore, it is important for both e-service providers and consumers to understand how the legal system handles service faults that result from using public e-services. When determining administrative accountability for damages inflicted on consumers of public e-services, the administrative judiciary makes a distinction between proven error, presumed error, and no error.

Study Problem:

Administrative liability, particularly administrative liability for electronic damages, has evolved toward compensating those harmed by administrative activity, requiring the presence of an element of fault for such liability to be established. The old principle was that the state was not liable for its harmful actions, given its authority and sovereignty, and that its liability was limited to exceptions. However, this changed as a result of the state's transformation from a guardian state to an intervening state in many activities that were previously the exclusive domain of individuals. As a result of the tremendous scientific and technological developments in all fields, and in connection with the state's practice of these activities, harm may be inflicted on individuals and those dealing with it without any fault being attributed to the administrative body. Given the inadequacy of the fault theory, the theory of objective administrative liability emerged, which does not require the element of fault and is satisfied with the two elements of damage and causation. It was therefore necessary to search for a legal basis for this liability, which is based primarily on consideration of the principle of justice and equality before public burdens. Hence, our current study seeks to answer the following question:

What is the legal basis upon which administrative liability for digital technical malfunctions is based?

Study Objectives:

Our current study seeks to achieve the following objectives:

- Understand the concept and principles of digital governance.
- Highlight the causes of digital technical failures.
- Understand the legal basis for management liability for digital technical failures.

Study Methodology:

The current study relies on an analytical approach to understand the concept and principles of digital governance, analyze the causes of digital technical failures, and determine the legal basis for management's liability for digital technical failures.

1. Digital Governance:

1.1. The Concept of Digital Governance:

Digitization is a modern concept that emerged with the emergence of information and communication technology, which resulted in a shift from using traditional methods of transmitting information and knowledge to using numbers to transmit this information and knowledge. The concept of digitization basically refers to taking theoretical information and encoding it into zeros so that computers can store, process and transmit it[1].

Digitization is defined as the social transformation resulting from the massive reliance on digital technologies to obtain, process, and share information. Thus, digitalization depends on the development of Internet access technologies and advanced software[2].

It is also known as the ability of a state and its people to use digital technologies to generate, process, and exchange information. Its concept is also linked to the concept that describes all of the social, economic, and political changes associated with the mass adoption of information and communications technology[3].

[1] Jason Bloomberg, Digitization and Digital Transformation: Confuse Them At Your Peril, 2018, P. 6.

[2] Raul Katz, Koutroumpis Pantelis, Measuring Socio - Economic Digitation A Paradigm Shift, U.S.A, 2012, P. 35.

[3] M Ruiz and Alejandra Soto, National Digital Strategy, National Digital Strategy Coordinator, Mexico, 2013, P. 13.

Accordingly, digital governance can be defined as the public sector's use of information and communications technology, including the Internet, mobile devices, and other tools, to improve and enhance the efficiency and effectiveness of providing information and services to citizens. Digital governance encourages active citizen participation[1].

1.2. The Importance of Digital Governance:

According to the World Bank (2002), the importance of digital governance is manifested in the following elements[2]:

- Simplifying the process of information accumulation for citizens and businesses.
- E-governance enables citizens to gather and access information related to government policies.
- Participation in the decision-making process.
- E-governance promotes democratic values by ensuring citizen participation at all levels in the governance process.
- E-governance automates various services and provides citizens with a surplus of information related to public welfare.
- E-governance ensures accountability and transparency in government transactions and public sector agencies.
- E-governance helps coordinate and monitor the activities of various government agencies.
- Proper implementation of e-governance helps citizens access public services online, thus saving citizens time and money from having to physically visit government offices.
- Adopting an e-governance policy is beneficial for the delivery of public services to citizens.

1.3. Principles of Digital Governance:

In the era of digital transformation, governments around the world are increasingly relying on information and communications technologies to provide more efficient and effective services to citizens. Digital governance is based on a set of fundamental principles that guide the digital transformation process and help achieve government goals. The basic principles of digital governance can be addressed as follows:

1.3.1. Transparency:

Transparency is one of the fundamental principles of digital governance. It refers to the provision of government information in an open and accessible manner to the public. The main goal of transparency is to reduce the gap between the government and citizens by disclosing all information related to government decisions and policies. In the digital age, the government can enhance transparency by using internet platforms and electronic portals to publish information related to government decisions, budgets, and public projects. This information can include details about general budgets, development plans, government policies, licenses, and government contracts. For example, the government can publish periodic reports on government projects, including the challenges they face and proposed solutions, which contributes to making the government process clearer to citizens[3].

Transparency contributes to building trust between the government and citizens. Transparency also contributes to reducing corruption, as it is difficult for officials to hide any information from the public under modern digital

[1] Choa Tang and R. Murga Perumal, The Characteristics and Values of E - Governance and The Role of E - Democracy, International Journal of Humanities and Management Science, Vol. 1, Issue 1, 2013, P. 142.

[2] Aman Singh, E- Governance: Moving Towards Digital Governance, Vidya A Journal of Gujarat University, Vol. 2, Issue 1, January- June 2023, PP. 204- 215.

[3] OECD, The OECD Digital Government Policy Framework: Six dimensions of a Digital Government, OECD Public Governance Policy Papers, No, 02, OECD Publishing Paris, 2020.

systems. In addition, transparency opens the way for citizens to participate effectively in political life, as they can access information related to decisions that affect their lives[1].

Transparency is one of the most important principles of digital governance, as it relies on providing accurate and clear information about digital operations within the institution. Transparency enhances trust between public institutions and citizens, and reduces the chances of corruption and mismanagement. Transparency includes[2]:

- **Data availability:** Providing data and information in an open and easily accessible manner to all relevant parties, including employees, citizens, and stakeholders.
- **Performance reports:** Publish periodic reports that illustrate the performance of digital systems and technology projects, focusing on results and challenges.
- **Clarity in decisions:** Ensuring that decisions related to digital transformation are based on clear and understandable data.

1.3.2. Accountability:

The principle of accountability refers to the commitment of government institutions to provide clear and convincing explanations and answers to citizens about the decisions and actions taken. This principle enhances citizens' ability to hold the government accountable for its performance and actions. Digital governance contributes to enhancing accountability by providing electronic platforms that allow citizens to submit complaints and suggestions[3]. For example, citizens can submit complaints about government services online, and then track the status of the complaint until it is resolved. The government can also provide periodic reports on how public policies are implemented and the overall performance of government institutions. In some cases, technologies such as blockchain can be used to ensure transparency and accountability in government operations, as every government process can be tracked from start to finish[4].

By strengthening accountability, government performance can be improved, as officials are assured that they will be subject to continuous review by citizens. Accountability also contributes to strengthening trust between government and citizens, as citizens feel that the government is accountable for its actions. Accountability is also an effective tool for reducing corruption, as it makes it difficult for officials to evade responsibility. Accountability ensures that digital decisions are based on sound foundations, and that performance is continuously improved. It means holding individuals and teams accountable for the results of their work within the framework of digital operations. Accountability includes[5]:

- **Defining roles and responsibilities:** Clearly defining the roles and responsibilities related to managing technology and digital systems within the organization.
- **Monitoring mechanisms:** Establishing control systems that enable performance monitoring and assessing compliance with established standards and policies.

---

[1] Yannis Charalabidis, Leif Flak and Gabriela Pereire, Scientific Foundations of Digital Governance and Transformation Concepts, Approaches and Challenges, Springer Publisher, 2022, P. 102.

[2] Jopang Jopang, Septian Aryatama, Muazzinah Muazzinah and Qamal Qamal, Exploring the Relationship Between E-Government, Transparency, and Citizen Trust in Government Services, Global International Journal of Innovative Research, Vol. 2, Issue. 6, July 2024, PP. 1354- 1363.

[3] Irfan Bora, Huijue Kelly Duan and Miklos A, Vasarhely, Chanyuan Zhang and Jun Dai, The Transformation of Government Accountability and Reporting, Journal of Emerging Technologies in Accounting, Vol. 18, Issue. 2, 2021, PP. 1- 21.

[4] Mohammad Mustafa Ibrahimy, Alex Norta and Peeter Normak, Blockchain-Based Governance Models Supporting Corruption-Transparency: A Systematic Literature Review, Blockchain Research and Applications, Vol. 5, Issue 2, December 2023, PP. 1- 21.

[5] Kelsie Nabben and Primavera De Filippi, Accountability Protocols? On - Chain Dynamics in Blockchain Governance, Internet Policy Review, Journal of Internet Regulation, Vol. 13, Issue. 4, October 2024, PP. 1- 22.

- **Sanctions and rewards:** Implementing a system of rewards and sanctions based on performance, which encourages adherence to established standards.

1.3.3. Efficiency:

In digital governance, efficiency means using available resources effectively to achieve specific goals while minimizing waste of time and money. Efficiency aims to improve the quality of government services and reduce costs, which contributes to providing better services to citizens. Efficiency can be achieved in public institutions through the implementation of advanced digital systems such as process automation, the use of artificial intelligence technologies, and big data analysis[1]. For example, the efficiency of government service delivery can be improved by creating digital platforms that enable citizens to complete their transactions faster and more accurately, such as submitting government applications or receiving documents. In addition, digital systems contribute to improving the use of human resources by improving recruitment and training processes, which reduces errors and increases the speed of decision-making.

Achieving efficiency leads to improved government performance and reduced costs. When public institutions use resources effectively, they can provide better and faster services to citizens. For example, when applying for licenses, the time required for these procedures can be reduced by digitizing the entire process, reducing the need for staff and increasing the speed of implementation[2].

1.3.4. Justice and Equality:

Justice and equality are fundamental pillars of digital governance, ensuring equal opportunities for all individuals to access and benefit from government services without discrimination. Achieving digital justice requires ensuring equitable access to technology and digital resources for all segments of society, regardless of their economic, social, or geographic backgrounds. Digital transformation should be a tool for promoting equality among citizens, not a factor that exacerbates existing gaps[3].

Providing a fair digital environment includes designing efficient and transparent e-government services that are accessible to all citizens without exception. To achieve this, public institutions must develop policies that ensure the equitable distribution of digital infrastructure, including high-speed internet, technological devices, and interactive digital platforms. Justice here does not only mean equal access, but also extends to ensuring the equal quality of services provided, ensuring no discrimination in the level of service between urban and rural areas or between different groups[4].

Justice in digital government also requires protecting users' rights by ensuring respect for their privacy and the security of their data. This includes establishing strict regulations that protect individuals from digital exploitation and ensure their data is used in a transparent and responsible manner. When citizens trust that their data is protected, they become more willing to use digital services, which enhances the effectiveness of digital transformation and increases their interaction with the government's digital ecosystem. Achieving equality in digital governance also means removing barriers that may prevent some groups from benefiting from digital services. It is

[1] Vincent J. Straub, Youmna Hashem, Jonathan Bright, Satyam Bhagwanani, Deborah Morgan, John Francis, Saba Esnaashari and Helen Margetts, AI for bureaucratic productivity: Measuring the potential of AI to help automate 143 million UK government transactions, March 2024, PP. 1- 18.

[2] Deloitte, AI: Can smart technologies drive government efficiency?, Available at: https://www.deloitte.com/us/en/Industries/government-public/articles/ai-in-federal-government.html.

[3] Gatot Hery Djatmiko, Obsatar Sinaga and Suharno Pawirosumarto, Digital Transformation and Social Inclusion in Public Services: A Qualitative Analysis of E-Government Adoption for Marginalized Communities in Sustainable Governance, Sustainability, Vol. 17, Issue 7, 2025, PP. 3- 4.

[4] Meena Chary, Social Equity, the Digital Divide and E-Governance: An Analysis of E-Governance Initiatives in India, University of South Florida, USA, 2011, P. 65.

essential that government platforms are easy to use and accessible to everyone, including the elderly and people with disabilities. This can be achieved by designing interactive digital interfaces that rely on assistive technologies such as text-to-speech, or providing options to display content in ways that suit the needs of different users[1].

1.3.5. Innovation and Development:

Innovation and development are essential elements for achieving effective and sustainable digital governance. They contribute to improving the quality of government services, enhancing operational efficiency, and providing smart solutions that meet citizens' changing needs. Innovation in digital governance relies on the use of modern technologies such as artificial intelligence, big data analytics, and the Internet of Things to improve decision-making processes and deliver smoother and more efficient services[2].

Developing digital infrastructure is a priority in this context, as it ensures an advanced environment capable of absorbing and effectively implementing technological innovations. This includes improving communication networks, creating interactive digital platforms, and adopting cloud computing systems that facilitate the exchange of various information, contributing to the provision of interconnected and responsive government services. Innovation in digital governance is not limited to developing technologies, but extends to redesigning administrative policies and procedures in a way that contributes to facilitating operations and improving the user experience. This can be achieved by adopting smart management methods and developing systems that enable citizens to interact with government institutions easily, such as smartphone applications that provide integrated digital government services[3].

Furthermore, investing in human capital is a fundamental pillar of digital governance development, as digital transformation requires qualified personnel capable of managing and continuously developing modern technologies. Therefore, specialized training programs must be provided, and partnerships with universities and research institutions must be strengthened to support innovation and develop technical solutions that meet societal needs. Furthermore, public-private sector collaboration plays a significant role in accelerating digital innovation. Through strategic partnerships, governments can leverage the technical expertise provided by specialized companies, contributing to the development of more efficient and innovative services and enhancing investments in digital infrastructure. Innovation and development are therefore the cornerstone of successful digital governance, enabling the provision of advanced government services, enhancing transparency, and achieving sustainability through adopting an innovation-driven approach. This improves government performance, enhances citizen engagement, and builds an advanced digital society that keeps pace with modern developments[4].

1.3.6. Participation and Cooperation:

Participation plays a fundamental role in strengthening digital democracy, as it allows individuals the opportunity to express their opinions and contribute to the development of public services and policies. Digital governments provide tools such as electronic referendums, suggestion platforms, and virtual dialogues, allowing citizens to interact directly with decision-makers and contribute to improving government performance[5]. Cooperation is a vital element in the success of digital governance, as it relies on the integration of efforts between the public and private

[1] Olga Kolotouchkina, Carmen Llorente Barroso and Juan Luis Manfredi Sanchez, Smart Cities, The Digital Divide and People With Disabilities, Cities, Vol. 123, April 2022, PP. 1- 4.

[2] OECD, Enabling Digital Innovation in Government: The OECD GovTech Policy FrameworK, 2024, PP. 12- 13.

[3] Abdullah M. Al-Ansi, Askar Garad, Mohammed Jaboob and Ahmed Al-Ansi, Elevating E -Government: Unleashing The Power of AI and IoT for Enhanced Public services, Heliyon Journal, Vol. 10, 2024, PP. 10- 11.

[4] Marijn Janssen, Martijn Hartog, Ricardo Matheus, Aaron Yi Ding, George Kuk, Will Algorithms Blind People? The Effect of Explainable AI and Decision-Makers' Experience on AI Supported Decision-Making in Government, Soc. Sci. Comput. Vol. 40, Issue 2, 2022, PP. 478–493.

[5] Anni Jäntti, Henna Paananen, Anna-Aurora Kork and Kaisa Kurkela, Towards Interactive Governance: Embedding Citizen Participation in Local Government, Administration and Society Journal, Vol. 55, Issue 8, June 2023, PP. 1529- 1554.

sectors, academic institutions, and civil society. By building strategic partnerships, innovative digital solutions can be developed that meet the changing needs of society, enhance the efficiency of government services, and provide an integrated technical environment that enables the exchange of knowledge and expertise[1].

In addition, international cooperation in the field of digital governance contributes to the exchange of best practices, the promotion of technological development, and the ensuring that digital systems comply with global standards by engaging in international cooperation networks. Governments can improve their digital policies and benefit from global expertise in the fields of cybersecurity, data management, and artificial intelligence. Therefore, activating participation and cooperation has a positive impact on the digital economy, as it allows startups and entrepreneurs to contribute to the development of government services by providing innovative digital solutions. This approach also enhances a competitive environment that contributes to improving the quality of services and creating new job opportunities in the fields of technology and innovation. In addition, participation and cooperation are two essential pillars of the success of digital governance, as they contribute to enhancing interaction between governments and societies, achieving transparency, and improving the services provided by involving everyone in the digital transformation process[2].

1.3.7. Compliance With Laws and Regulations:

Compliance with laws and regulations is a fundamental principle of digital governance, ensuring that public and private institutions adhere to the legal and regulatory standards governing digital operations. This compliance aims to achieve transparency, enhance trust in digital services, and protect the rights of individuals and institutions, contributing to building a safe and sustainable digital environment. Digital compliance requires adherence to legislation related to the protection of personal data, such as privacy laws that ensure that information is not misused or leaked. Compliance also includes cybersecurity regulations that aim to protect digital systems from cyberattacks and potential breaches, thus maintaining the stability of the digital infrastructure and ensuring the continuity of government services[3].

Furthermore, compliance with laws and regulations includes following international and local standards governing areas such as electronic transactions, digital signatures, and artificial intelligence, to ensure integration and compatibility with global digital systems. This commitment contributes to facilitating international cooperation and enhancing investment opportunities in the digital economy by building a clear and stable legal environment. Compliance also requires digital institutions to adopt strict internal policies to ensure continued compliance with legal systems, such as conducting periodic audits, updating security procedures, and providing ongoing training for employees on new digital laws. This contributes to reducing legal risks and enhancing institutions' ability to adapt to technological and legislative changes[4].

Furthermore, compliance enhances citizens' trust in digital services, as users realize that their data and rights are protected by clear and enforceable laws. It also ensures the provision of fair and reliable digital government services, which enhances individual participation in the digital ecosystem and contributes to a successful digital transformation. Compliance with laws and regulations also ensures the legal sustainability of digital technologies, protects the rights of individuals and institutions, and enhances the reliability of digital systems. Through strict

[1] Liang Ma, Tom Christensen and Yueping Zheng, Government Technological Capacity and Public–Private Partnerships Regarding Digital Service Delivery: Evidence From Chinese Cities, International Review of Administrative Sciences, Vol. 89, Issue. 1, June 2021, P. 5.

[2] Els M. Leclercq and Emiel A. Rijshouwer, Enabling Citizens' Right To The Smart City Through The Co-Creation of Digital Platforms, Urban Transformations, March 2022, PP. 1-19.

[3] Patrick Spencer, Data Governance and Digital Transformation in the Public Sector, Kiteworks, September 2024, Available at: https://www.kiteworks.com/cybersecurity-risk-management/data-governance-in-the-public-sector/.

[4] Leah Sadoian, Guarding Governance: Cybersecurity in the Public Sector, 2025, Available at: https://www.upguard.com/blog/cybersecurity-in-the-public-sector.

adherence to the legal framework, governments can achieve a safe and orderly digital transformation that enhances economic and social development[1].

1.3.8. Security and Data Protection:

Security and data protection refer to the need to protect personal data and sensitive information collected by public institutions, and to ensure that this data is protected from cyber threats and attacks. Digital governance requires that public institutions follow the best standards to ensure data protection. This is achieved by using advanced encryption technologies and modern security systems to protect personal information. Public institutions must also comply with local and international regulations related to data protection, such as the General Data Protection Regulation (GDPR)[2]. In addition, employees must be trained on how to handle sensitive data and develop strict policies to control access to information. Implementing security standards reduces the risks associated with cyber-attacks and data leaks. It also enhances citizens' confidence in the digital system, as they feel their personal information is well protected. Security and data protection also contribute to enhanced compliance with local and international privacy laws[3].

Cybersecurity is a fundamental pillar of digital governance, aiming to protect data and digital systems from cyber threats. It also ensures business continuity and protects an organization's reputation from damage resulting from cyberattacks. Cybersecurity principles include implementing strict measures to protect personal and sensitive data from breaches or leaks, identifying potential cyber risks and developing proactive plans to address them, and providing employee training programs to raise their awareness of the importance of cybersecurity and how to deal with threats[4].

1.3.9. Sustainability:

Sustainability in digital government means ensuring the long-term sustainability of digital improvements, including the sustainability of technology, financial resources, and human resources. Sustainability is achieved by adopting long-term strategies for developing digital technology in public institutions. This includes ensuring that digital systems are scalable and keep pace with future technological developments. Digital infrastructure must also be sustained through regular hardware and software updates[5]. Additionally, employees must be continuously trained in the use of these technologies to ensure continued efficiency in delivering digital services. Sustainability ensures the continuity of digital improvements in the future, making government services more effective in the long term. Adopting sustainable digital solutions also helps reduce the environmental impact by reducing the need for paper and other physical resources[6].

Sustainability, as a fundamental principle of digital governance in public institutions, ensures that digital operations are effective and aligned with environmental and social objectives through the efficient use of technological resources. Sustainability principles include rationalizing consumption, using energy and technological resources

[1] Sarah Lee, Digital Governance Essentials: Navigating Ethics in Public Administration for a Digital Age, May 2025, Available at: https://www.numberanalytics.com/blog/digital-governance-essentials.

[2] Dawit Negussie, Importance of Cybersecurity Awareness Training for Employees in Business, Peer Reviewed, Multidisciplinary & Multilingual Journal, Vol. 2, Issue 2, July- December 2023, PP. 104- 107.

[3] S. Al Fadhli, Challenges of Digital Transformation in Libyan Education. International Journal of Education and Information Technologies, 2021, P. 61.

[4] C. V. Govindraj, Digital Governance and Cybersecurity: Challenges in the age of E- Governance, Journal of Visual and Performing Arts, Vol. 5, Issue. 1, January 2024, PP. 4328- 4332.

[5] Noella Edelmann and Shefali Virkar, The Impact of Sustainability on Co-Creation of Digital Public Services, Administrative Sciences, Vol. 13, Issue 1, 2023, PP. 13- 14.

[6] Mohammed Ibrahim Gariba, Emmanuel Ebo Arthur and Samuel Amponsah Odei, Assessing the impact of public digitalization on sustainability: the mediating role of technological innovation in the context of the EU, Discover Sustainability, 2024, PP. 5-6.

effectively to reduce waste, developing long-term strategic plans to ensure the continuity of digital operations, and reducing the environmental impact of digital operations through the use of environmentally friendly technologies[1].

2. Digital technical failures:

2.1. Definition of Digital Technical Failures:

Digital technical failures are defined as a failure in information technology systems that causes the system to be inconsistent with the planned reality or unable to perform its intended functions. These failures are the result of gaps between design and reality, poor project management, or the lack of an appropriate technical environment[2]. These failures result in systems being shut down or partially or completely destroyed. Digital technical failures can be classified as[3]:

- **Development defects:** Human errors in design or coding.
- **Material defects:** Equipment malfunctions.
- **Interaction defects:** Problems connecting components or interfaces.
- **Natural defects:** Such as natural disasters.

2.2. Causes of digital technical failures:

There are several reasons for digital technical failures, including:

2.2.1. Inadequate System Requirements Engineering:

Requirements engineering is the process of discovering, documenting, and analyzing the services that a particular system will provide. This process involves systematic research and study of systems, processes, materials, operating environments, user needs, and other elements and materials to determine the needs of the new system[4]. Inadequate system requirements specifications cause 50% of the failures of e-government information systems projects in developing countries. For example, the student information system implemented by the Uganda Management Institute (UMI) failed because it omitted vital features in the finance module. The analyst did not include the requirements for these features in the initial requirements specification document[5].

2.2.2. Inadequate Project Management:

Project management is the application of knowledge, skills, tools and techniques to direct project activities in line with its goals and objectives. Many e-government information systems projects fail due to poor project management. An example of this is the failure of the Electronic National Traffic Information System (E-NaTIS) in South Africa, according to the African Journal of Information and Communication (AJIC), mainly due to poor

[1] Apurva Goel, Snehal Masukar and Girish R. Pathade, An Overview of Digital Transformation and Environmental Sustainability: Threats, Opportunities and Solutions, Sustainability Journals, Vol. 16, Issue 24, PP. 7-8.

[2] Leonidas Anthopoulos, Christopher G. Reddick, Irene Giannakidou and Nikolaos Mavridis, Why e-government projects fail? An analysis of the Healthcare.gov website, Government Information Quarterly Journal, Vol. 33, Issue 1, January 2016, P. 165.

[3] Baseer Ahmad Baheer, David Lamas and Sónia Sousa, A Systematic Literature Review on Existing Digital Government Architectures: State-of-the-Art, Challenges, and Prospects, Administration Sciences Journal, 2020, P. 1.

[4] S. Ullah, M. Iqbal and A. M. Khan, A Survey on Issues in Non - Functional Requirements Elicitation. In Proceedings of International Conference on Computer Networks andInformation Technology, Islamabad, 11- 13 July 2011, PP. 333- 340.

[5] Rehema Baguma and Jude Lubega, Factors for success and failure of e-government projects. In ICEGOV'13: Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance, 2013, PP. 194- 197.

project management[1]. Therefore, e-government projects must adopt proven management methodologies, align their objectives with the strategic goals of the organization, and employ their competence to manage them[2].

2.2.3. Missing or Incomplete Features:

An IS project is said to be successful if it is delivered on time and within the specified budget and with the required quality, features, and ease of use that reflect the real needs of the clients or users[3]. In some cases, e-government IS projects are delivered and accepted with vital missing or incomplete features, thus failing to work and achieve the expected results[4]. This practice leads to the total or partial failure of the e-government IS project. For example, the "Gorilla Buddy" project in Uganda, which was implemented to raise awareness and funds to promote gorilla conservation, was implemented without the essential features of selling promotional materials online and befriending gorillas via SMS[5]. Many reasons can lead to the delivery of incomplete projects, including government officials' resignation due to corruption and failure to follow proper procedures[6].

2.2.4. Inadequate Project Planning:

A project plan identifies activities, timelines, resources, risks, constraints, expected deliverables, and baseline information against which the project can be implemented, monitored, and evaluated[7]. Many of the challenges faced by e-government projects can be avoided or mitigated if carefully planned[8]. The e-Revenue Licensing Project in Sri Lanka is considered a successful e-government initiative due to its good planning[9].

2.2.5. Inappropriate Technology Selection:

When selecting technology for a particular project, several factors must be considered, including ease of learning and use, fitness for purpose, ease of integration with existing systems, availability of documentation and support, availability of skills, overall implementation costs, and overall perceived quality and usefulness[10]. Factors such as corruption may influence technology selection, leading to what are commonly known as vendor-led projects. The smart card project in Thailand is an example of the use of inappropriate technology in an e-government initiative[11].

2.2.6. Insufficient Senior Management Support:

[1] Mustafa Afyonluoğlu, Atilla Aydin Sare Gul Sevil, Eda Yüksel and Murat K. Güngör, An E-Government Project Management Approach with E- Transformation Perspective, International Journal of E Business and E Government Studies, Vol. 6, Issue 1, 2014, PP. 21- 33.

[2] Jayantha Rajapakse, Abraham Gert Van der Vyver and Erin Hommes, E- Government Implementations in Developing Countries: Success and Failure, Two Case Studies, IEEE International Conference on Information and Automation for Sustainability, 27- 29 September 2012, PP. 95- 100.

[3] Ramlah Hussein, Nor Shahriza Abdul Karim and Mohd Hasan Selamat, The Impact of Technological Factors on Information Systems Success in The Electronic Government Context, Business Process Management Journal, Vol. 13, Issue 5, September 2007, PP. 613- 627.

[4] Isaac Sakyi Damoah and Cynthia Akwei, Government Project Failure in Ghana: A Multidimensional Approach, International Journal of Managing Projects in Business, Vol. 10, Issue 1, 2017, PP. 32- 59.

[5] Baguma and Lubega, Op, Cit, PP. 194- 197.

[6] Damoah and Akwei, Op, Cit, PP. 32- 59.

[7] Pierre Bakunzibake, Ake Grönlund and Gunnar O. Klein, E- Government Implementation in Developing Countries: Enterprise Content Management in Rwanda, Electronic Government and Electronic Participation, February 2018, PP. 251- 259.

[8] Amirhossein Ghapanchi, Zarei Behrouz and Amir Albadvi, Framework for E - Government Planning and Implementation, Electronic Government An International Journal, Vol. 5, Issue 1, January 2008, PP. 71- 90.

[9] Rajapakse, Op, Cit, PP. 95- 100.

[10] Hussein et al, Op, Cit, PP. 613- 627.

[11] Damoah and Akwei, Op, Cit, PP. 32- 59.

Senior managers are expected to closely monitor critical aspects of the project, including ensuring that the project's goals, objectives, vision, and values reflect the organization's values. Senior managers must ensure that the project is managed according to the organization's standards, and that resources are provided in a timely manner. They must also ensure that project risks are adequately identified and mitigated. A systematic project review will ensure that key milestones are completed on time and that project resources are utilized optimally. Finally, senior managers must promote the project to internal and external stakeholders[1].

2.2.7. Integration Failure:

Providing e-government services requires vertical and horizontal integration of e-government systems[2]. Given the difficulty of achieving this, the challenges of e-government integration are classified into four main categories: strategy, technology, policy, and organization[3]. Most government institutions and agencies develop their e-government systems independently of each other, without paying much attention to how other government institutions and agencies interact with them[4]. For example, the integration between the Citizen Assistance Request (CHR) system, designed by the Bangladesh Police to facilitate online incident reporting, and the identification system to verify the identity of applicants failed due to technical and organizational issues. As a result, the police continued to receive applications with fake names and contact addresses[5].

2.2.8. Disadvantages of Procurement and Contracts:

Government agencies outsource most e-government information systems projects to third parties through legally binding contracts[6]. In some cases, they use various forms of public-private partnerships. In both cases, a contract is essential that defines the parties involved, their obligations, the consequences of non-fulfillment, and dispute resolution procedures. The lack of a fair contract can lead to legal problems, which may ultimately lead to the failure of the project[7].

2.2.9. Inadequate Business Process Management (BPM):

Business Process Management (BPM) is an organizational strategy for identifying, modeling, analyzing, measuring, automating, optimizing, and continuously improving core activities in an organization[8]. The overall goal of e-government initiatives is to improve public service delivery and enhance management processes through electronic services. In this case, BPM and e-government are two complementary initiatives that should go hand in hand. Unfortunately, most e-government information systems projects are designed without including BPM as a core

[1] Shashank Ojha and I. M. Pandey, Management and Financing of E - Government Projects in India: Does Financing Strategy Add Value?, IIMB Management Review, Vol. 29, Issue 2, 2017, PP. 1- 19.

[2] Karen Layne and Jungwoo Lee, Developing Fully Functional E - Government: A Four Stage Model, Government Information Quarterly, Vol. 18, Issue 2, PP. 122- 136.

[3] Wing Lam, Barriers to e-government integration, Journal of Enterprise Information Management, Vol. 18, Issue 5, 2005, PP. 511- 530.

[4] Zuhoor Abdullah Al-Khanjar, Nasser Al-Hosni and Naoufel Kraiem, Developing A Service Oriented E - Government Architecture Towards Achieving E - Government Interoperability, International Journal of Software Engineering and Its Applications, Vol. 8, Issue 5, 2014, PP. 29- 42.

[5] Mohammad Mahmudul Hasan, E- Government Success and Failure: A Case Study of Bangladesh Police, Daffodil International University Journal of Science and Technology, Vol. 10, Issue 1, 2015, PP. 61- 67.

[6] Ojha and Pandey, Op, Cit, PP. 1- 19.

[7] Afyonluoğlu et al, Op, Cit, PP. 21- 33.

[8] Peter Trkman, The Critical Success Factors of Business Process Management, International Journal of Information Management, Vol. 30, Issue 2, 2010, PP. 125- 134.

component. Implementing an e-government information system without reengineering processes can lead to undesirable results and ultimately project failure[1].

2.2.10. Inadequate IS Testing:

Information systems testing is a critical phase in the system development life cycle[2]. It aims to verify, validate, detect, and fix system errors. During the verification process, the developed system is examined to assess its compliance with specified requirements. Inadequate system testing results in its inability to meet the expectations and needs of stakeholders, leading to its abandonment[3].

2.2.11. Inadequate Change Management:

E-government projects are transformational projects that tend to alter business processes, service delivery mechanisms, and organizational structure[4]. Successful transformation requires an appropriate change management process. Some e-government projects fail because the organization is unable to make the necessary institutional changes to transition from legacy processes to the new processes enabled by advanced e-government information systems. A practical change management framework must address all aspects of the organization's implementation, including technology, management, operations, legislation, personnel, and organization[5].

2.2.12. Staff and Skills Shortages:

An effective e-government implementation team must possess core skills, including strategic IT skills, information society skills, information management skills, technical skills, project management skills, and communication skills[6]. Most governments in developing countries suffer from a severe shortage of skilled personnel, and the lack of of relevant technical skills within the e-government project team negatively impacts the quality of information systems[7].

2.2.13. Excessive Technical Complexity:

Technical complexity refers to the difficulty of solving a particular problem using the relevant technology[8]. This includes the inability to accurately define information and processing requirements, data communications, and overall system design, setup, and configurations. Lack of thorough technical evaluation is a major cause of complexities and technical problems in e-government information systems projects. Learning from the mistakes of previous projects is critical to reducing risks and failures in new projects[9].

---

[1] Rodrigo L. Martin and Jorge M. Montagna, Business Process Reengineering Role in Electronic Government, The Past and Future of Information Systems: 1976–2006 and Beyond, Conference Paper, 21-23 Augst 2006, PP. 77- 88.

[2] Tomi Rajala and Hannes Aaltonen, Reasons for The Failure of Information Technology Projects in the Public Sector, In Book: The Palgrave handbook of the public servant, Palgrave MacMillan, May 2020, PP. 1- 21.

[3] Sarika Chaudhary, Latest Software Testing Tools and Techniques: A Review, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 7, Issue 5, 2017, PP. 538- 540.

[4] Afyonluoğlu et al, Op, Cit, PP. 21- 33.

[5] Janja Nograsek, Change Management as a Critical Success Factor in E - Government Implementation, Business Systems Research Journal, Vol. 2, Issue 2, September 2012, PP. 13- 24.

[6] M. Al Slami, S. Mohtar and N. Hasnan, Skills and Factors of E - Government: Case Study of Sultanate of Oman, International International Journal of Innovation, Management and Technology, Vol. 8, Issue 4, PP. 313- 319.

[7] Ghapanchi et al, Op, Cit, PP. 71- 90.

[8] Alexei Botchkarev and Patrick Finnigan, Complexity in The Context of Information Systems Project Management, Organizational Project Management, Vol. 2, Issue 1, 2015, PP. 15- 34.

[9] Indranil Mukherjee, Understanding Information System Failures from The Complexity Perspective, Journal of Social Sciences, Vol. 4, Issue 4, 2008, PP. 308- 319.

2.2.14. Outdated Technology:

Planning and implementing government systems projects takes a relatively long time, and as a result, some e-government projects are implemented while the associated technologies are obsolete or on the verge of becoming obsolete. Developing countries also suffer from the adoption of outdated technologies when developed countries donate technological equipment and systems[1].

2.2.15. Information Gaps:

A mismatch between what is captured or produced by the system and what is requested by system users can lead to the failure of an e-government information system. Information gaps in an e-government information system occur in three situations: capturing information that is not necessary for processing or reporting; failing to capture essential information needed for processing or reporting; and requesting certain information that may not be available or relevant to certain users or scenarios[2]. For example, the Citizen Assistance Request (CHR) system designed by the Bangladesh Police required a valid signature from the requester to initiate an investigation. However, the inability of citizens to provide digital signatures online rendered the system unusable[3].

2.2.16. Inadequate Infrastructure:

E-government infrastructure includes hardware platforms, software platforms, middleware, data communications equipment, networks, backup devices, disaster recovery devices, and security technologies. These devices and equipment enable the provision of e-government services that are easily accessible to users. In the field of information technology, the performance and effectiveness of infrastructure are measured in terms of reliability, which is its ability to ensure continuity of operation; scalability, which is its ability to accommodate increased loads; and flexibility, which is its ability to accommodate changes that may be required[4].

2.2.17. Political interference:

Governments are run by politicians who influence many aspects of decision-making, leadership, and development initiatives. Politicians influence many government projects, both positively and negatively, through various means, such as appointing project managers, manipulating their scope and outcomes to suit their political interests, and making different decisions[5]. When a digital project is imposed for political purposes or without adequate technical preparation, this leads to unjustified acceleration of the project stages, leading to the project's failure[6].

2.2.18. Inappropriate Organizational Structure:

Government institutions are built to support their core missions. They rely on a hierarchical structure with bureaucratic leadership, close relationships, and strict rules and procedures. The organizational structure is a fundamental element of e-government governance. Poor allocation of responsibilities or lack of coordination among project stakeholders leads to conflicting decisions and delays in resolution. Therefore, institutions

[1] Jens Goedeke, Mario Mueller and Oleg Pankratz, Uncovering the Causes of Information System Project Failure, In AMCIS 2017 proceedings, 2017, PP. 1- 10.

[2] Vivek Vyas, Shivani Vyas and Amit Kundan, Management Information System: Information Needs of organization, International Journal of Information and Computation Technology, Vol. 4, Issue 17, January 2014, PP. 1903- 1908.

[3] Hasan, Op, Cit, PP. 61- 67.

[4] Deepak Dahiya and Saji Mathew, IT Infrastructure Capability and E - Government System Performance: An Empirical Study, Transforming Government People Process and Policy, Vol. 12, Issue 2, January 2018, PP. 16- 38.

[5] Rajala and Aaltonen, Op, Cit, PP. 1- 21.

[6] Asad Abbas, Ali Faiz, Anam Fatima and Ander Avdic, Reasons for The Failure of Government IT Projects in Pakistan: A contemporary Study, International Conference on Service Systems and Service Management, 16- 18 June 2017, PP. 1-6.

implementing e-government initiatives must make the necessary reforms to accommodate and manage changes in the e-government system[1].

2.2.19. Security Reasons:

which are represented by the management's failure to protect data from internal and external manipulation and fraud, in addition to cybersecurity risks, security breaches, and unauthorized access[2].

3. Foundations of Administrative Responsibility For Digital Technical Malfunctions:

An important development meant to improve efficiency and service delivery is the use of electronic public administration in the management of public facilities. However, there are dangers associated with this shift that could negatively impact beneficiaries, hence a legal framework for state culpability is required. Three main areas are examined in this analysis of the foundation of administrative responsibility in the context of electronic public facilities: strict liability (without error), liability based on proved error, and liability based on presumed error.

3.1. Verified Error:

Verified Conventional administrative liability is predicated on the existence of fault, which is usually demonstrated by an error. This idea applies to circumstances in the field of electronic public administration where the administration's actions—like system failures or data breaches—directly arise from observable errors. For example, the administration may be responsible for damages if a coding error causes a public facility's digital system to process personal data incorrectly, causing harm. This is consistent with the idea that the state bears responsibility for any illegal or irregular official conduct carried out while performing its obligations.

French administrative law provides a seminal illustration of this type of fault-based liability, since the Conseil d'État has repeatedly maintained that a public organization is accountable for "faute de service," or a service error, if a public system malfunctions and harms people[3].

This kind of accountability serves as a legal incentive for public entities to responsibly maintain and improve their information systems in addition to being necessary for redress[4]. Furthermore, under frameworks like the EU General Data Protection Regulation (GDPR), proved mistakes in the management of personal data may potentially result in administrative punishment and civil compensation[5]. Administrative liability for digital mismanagement, therefore, is a contemporary extension of long-standing public law principles under the notion of demonstrated fault, guaranteeing that technology advancement does not evade established norms of accountability.

It is essential to realize that, despite having legal identity, the administration lacks a will separate from its agents. Since public officials are the means by which the administration functions, mistakes made in the performance of

[1] Rogers Matte, Bureaucratic Structures and Organizational Performance: A comparative Study of Kampala Capital City Authority and National Planning Authority, Journal of Public Administration and Policy Research, Vol. 9, Issue 1, PP. 1- 16.

[2] Nonye Aniefiok Asikpo, Impact of Digital Transformation on Financial Reporting in the 21st Century. International Journal of Comparative Studies and Smart Education, Vol. 1, Issue 1, 2024, PP. 34- 45.

[3] Conseil d'État, Dame Veuve Muësser, CE, France, 20 November 1946, Rec. Lebon, 252.

[4] David H. Rosenbloom, Public Administration: Understanding Management, Politics, and Law in the Public Sector, 9th ed, McGraw-Hill Education, New York, 2022, PP. 284–285

[5] Paul De Hert and Vagelis Papakonstantinou, The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?, Computer Law & Security Review, Vol. 32, Issue. 2, 2023, PP. 179–194.

administrative duties are thereby committed by them[1]. Due to this issue, the French Conseil d'État created a crucial legal theory that distinguishes between service fault (faute de service) and personal fault (faute personnelle)[2].

3.1.1. Personal Fault Versus Service Fault:

In civil responsibility, the individual is usually held directly responsible for the fault. But according to administrative law, personal culpability describes actions taken by a public servant that are completely unrelated to their administrative role, such as behavior resulting from personal hostility, willful misbehavior, or actions taken outside the parameters of their job. In these situations, the individual bears responsibility, and the regular civil courts have jurisdiction[3]. On the other hand, even if the act was careless or damaging, misconduct that occurs while carrying out official tasks is considered a service fault. The administrative courts have the authority to consider such claims, and the administration is accountable for these actions. This distinction represents the understanding that although the administration should be held responsible for the actions of its agents, it should not be held liable for actions that are unrelated to public service or that gravely breach the position's duties.

The French administrative courts' jurisprudence, especially the Conseil d'État's rulings, has been a significant source of advice in this area. In the 1911 landmark decision Anguet CE, for example, the court recognized the potential for both forms of guilt to coexist and upheld the administration's liability even in cases where personal fault occurred, provided that the conduct was not completely separated from service. This dual culpability approach, which is becoming more widely recognized in different legal systems throughout the world, makes sure that victims are not left without compensation because of the difficulty of fault classification[4]. In conclusion, the contemporary theory of administrative accountability strikes a compromise between defending the rights of individuals injured by official activities and the protection of the public interest. Administrative law strengthens the rule of law in public administration by achieving both functional responsibility and justice in the distribution of culpability by differentiating between personal and service failures.

Though the distinction between faute personnelle (personal error) and faute de service (service fault) has long been acknowledged by the French administrative justice, it is still theoretically and practically challenging to distinguish between the two. The concept mostly depends on an abstract criterion that is hard to consistently apply in practical settings, despite the fact that its goal is to fairly divide blame between the administration and the public employee. The idea of fault, whether it be personal or service-related, is fundamentally human behavior, and its assessment is subject to a number of overlapping subjective and objective criteria. The difficulty stems from the fact that administrative errors are rarely the consequence of isolated incidents, but rather are frequently the consequence of intricate relationships between the psychological makeup of the employee, the institutional demands of the administrative setting, and more general social and cultural factors[5].

According to academics, a public employee's psychological composition may affect how they behave under pressure, in positions of authority, or within an institutional hierarchy, which can make it difficult to distinguish between an act that is completely personal and one that is ingrained in the workplace[6]. Furthermore, the employment environment—such as workload, administrative restrictions, or ambiguous procedural guidelines—may influence workers to make judgments that are debatably service-related even though they are faulty[7]. The justice and consistency of imposing personal accountability on an official whose actions, although possibly abnormal, were

[1] Peter Cane, Administrative Law, 6th ed, Oxford University Press, Oxford, 2021, P. 197.

[2] Louis Rolland and Pierre Jèze, Traité de droit administratif, 13th ed, Dalloz, Paris, 2022, P. 144.

[3] Georges Vedel and Pierre Delvolvé, Droit administratif, 12th ed, Presses Universitaires de France, Paris, 2021, PP. 312–314.

[4] Suzanne Tavares da Silva, Evolving Doctrines of State Responsibility: From Fault to Functionality, International Review of Administrative Law, Vol. 49, Issue. 2, 2023, PP. 205–228.

[5] Cane, Op, Cit, P. 192.

[6] Rolland and Jèze, Op, Cit, P. 151.

[7] Vedel and Delvolvé, Op, Cit, P. 329.

caused or made worse by systemic flaws are fundamentally called into question by this interaction. The French Conseil d'État's jurisprudence reflects this issue, as the courts have had trouble providing a clear and broadly applicable standard. In certain situations, judges focus on the employee's deliberate actions or the seriousness of their behavior; in other situations, they evaluate whether the act was naturally connected to the discharge of public obligations. This contradiction highlights a conflict between the legal reality that fault is frequently difficult to classify and the doctrinal aim to preserve a distinction for the purposes of assigning liability.

Though analytically helpful, this distinction should not exclude flexible judicial interpretation, according to modern administrative theory, particularly in cases where strict categorization could impede access to justice or equitable recompense[1]. Comparative jurisprudence, which includes developments in Germany and some common law systems, does, in fact, represent a trend toward emphasizing institutional accountability over personal blame, which lessens the severe effects of unduly strict fault distinctions[2].

Nonetheless, when a public official makes a mistake, courts must determine whether the error is personal, resulting from the employee alone, or a service error, for which the administration is accountable[3]. This distinction was established by the French Tribunal des conflits in the Pelletier case of 1873. The court determined that while a personal error made outside the purview of public duties makes the individual employee personally liable, a service error made while performing official duties entails the administration's liability[4]. However, this distinction's application is quite complicated. Being human, error is impacted by a variety of internal and external factors, including one's sociocultural background, work environment, and psychological makeup[5]. Because of this, developing a single standard to differentiate between the two kinds of error is challenging. As a result, the judge considers the particular facts, the circumstances, and the motivations behind the act before making a decision. A number of guiding standards have been proposed by courts and academics to help with this judicial evaluation:

- Misconduct in the official's private time is an example of a personal blunder that is obviously distinct from the job, both psychologically and physically.
- If an error is physically separated from official tasks, such as utilizing government equipment for personal wrongdoing, it is still regarded as personal even if it is mentally related to the job[6].
- If an error is physically separated from official tasks, such as utilizing government equipment for personal wrongdoing, it is still regarded as personal even if it is mentally related to the job[7]. In these situations, courts frequently examine the official's intentions or the gravity of the behavior[8].

Judicial practice has not established a single, abstract legal norm in spite of these conceptual parameters, and each case still depends on the factual matrix and judicial interpretation[9]. The practical fact that the distinction between personal and service fault is hazy and situation-specific is highlighted by this. Therefore, it is possible for a personal error to occur in an electronic public facility if an employee hacks into the site's security system on purpose or with extreme carelessness, causing the site to become completely paralyzed and its services to be suspended until repairs are made. Alternatively, the employee may disclose the confidentiality of personal information or tamper

[1] Suzanne Tavares da Silva, Fault or Function? Rethinking Administrative Responsibility in Modern Governance, International Review of Administrative Law, Vol. 50, Issue. 1, 2024, PP. 114–129.

[2] Giacinto della Cananea, Beyond the State: Public Liability in the European Union, European Public Law, Vol. 29, Issue. 2, 2023, PP. 187–205.

[3] Cane, Op, Cit, P. 198.

[4] Tribunal des conflits, Arrêt Pelletier, 30 July 1873, Rec, P. 546.

[5] Vedel and Delvolvé, Op, Cit, P. 312.

[6] Jean Waline, Droit administratif, 25th ed, LGDJ, Paris, 2023, P. 512.

[7] Vedel and Delvolvé, Op, Cit, P. 313.

[8] Cane, Op, Cit, P. 199.

[9] Rolland and Jèze, Op, Cit, P. 149.

with it by destroying or altering it, which would also be considered a crime known as illegal access to the automated data processing system.

However, according to the French State Council's approach of combining personal error and facility error, such personal errors do not prevent the administration's responsibility alongside the employee's responsibility by discovering the facility error in the simple failure to supervise the employee and take the necessary measures to prevent the occurrence of damage, or by the employee committing these personal errors while using the facility's means and tools. However, an electronic public facility may be held accountable for what is legally defined as a service error—an error that can be attributed to the management rather than a specific employee. This makes the administration liable under public law and requires it to use public funds to compensate the harmed party. The administrative judiciary, which has established specific criteria for detecting service faults, especially in the context of digitalized public services, has jurisdiction over such instances[1]. The legal doctrine acknowledges a variety of service error types, which are frequently categorized into three primary groups. According to the principles of administrative law of French provenance, each of these groups may carry particular liability implications, and this is becoming more prevalent in comparative public law systems:

- Failing to provide the Required Service:

This type of situation arises when the government does not offer a service that it is required by law to give. One example of such a failure in the context of electronic administration would be the inability to access an online government platform, the unresponsiveness of digital communication systems, or the lack of real-time access to public records that citizens are entitled to get[2]. The administration may be held liable under the laws governing public service liability if this failure harms a person or institution and is the consequence of carelessness, defects in the system's design, or inadequate technical maintenance. In these situations, the administration's systemic failure—which is manifested in its software planning, digital infrastructure, or incapacity to guarantee service continuity—causes the harm rather than a single human actor. This type of culpability is consistent with the more general concepts of objective fault in public administration, particularly in cases where the service is required and the user is harmed as a direct result of inaction. This type of issue highlights how public bodies are increasingly responsible for maintaining technological dependability and guaranteeing continuous access to e- government services, especially in cases when digital platforms take the role of more conventional, physical routes.

This type of administrative error can also occur when the administration declines to carry out a task that it is contractually or legally obligated to complete. In these situations, the administration's omission or abstention that causes harm to people establishes culpability rather than a positive conduct[3]. When an administration is legally required to take action but instead takes a passive or unjustifiable stance, this bad behavior is considered a service error under traditional administrative law. The courts have generally found that, where damage and a causal connection can be proven, failing to take action when it is due constitutes a breach of administrative duty and results in responsibility.

This type of liability is becoming more and more significant in the setting of computerized public administration. It could be demonstrated, for example, by a public servant not processing or transmitting a digital transaction after it has been completed, or by failing to receive a request that has been submitted electronically. In addition to modernizing public engagement, the automation and digitization of public services also entails legal requirements to preserve technological functionality and responsiveness. In the digital sphere, a refusal or failure to act might have the same legal repercussions as an express denial of service under traditional administration, especially when computers are supposed to operate independently or with little assistance from humans[4]. Therefore, the same

[1] Waline, Op, Cit, P. 523.

[2] Cane, Op, Cit, P. 207.

[3] Waline, Op, Cit, P. 524.

[4] Rolland and Jèze, Op, Cit, P. 143.

standards that apply to omissions in traditional administration must also be applied to electronic inaction, such as disregarded submissions, technical dead ends, or unanswered service requests. Therefore, if such inaction causes harm to a citizen and the other components of culpability (damage and causal linkage) are met, the state or administrative authority may be held accountable.

- Poor Public Service Performance:

This type of administrative error refers to situations in which the administrative body's performance of its responsibilities is subpar and causes harm to people. Poor service delivery or a lack of organization inside the facility may be the cause of these shortcomings. For instance, poor ventilation in offices, particularly when coal-burning devices are used for heating, can cause health problems for workers. Poor performance in the field of electronic public administration can take many different forms, but they all indicate a violation of the administration's duty of care to consumers of public digital services. In this case, the electronic public facility is accountable for the inability to maintain or arrange digital infrastructure, such as a poorly designed service platform with insufficient access points or complete functionality. A state or public organization may be held liable for misadministration if it offers few digital options that do not cover necessary services or does so in a way that is hazardous, unclear, or inaccessible[1].

Furthermore, systematic service faults may result from a lack of technical control, such as the failure to hire platform administrators, cyber security experts, or IT supervisors. These mistakes could put users at danger for things like account hacking, data breaches, or losing personal information, all of which the administration is required by law to avoid[2].

Administrative law philosophy and jurisprudence uphold the notion that the administration has accountability for systemic or organizational flaws that result in harm in addition to its deliberate or careless actions. Actionable faults under public service liability may include, in particular, poor application of electronic security standards, unclear platform instructions, poor management that permits unwanted access, or recurring technical errors.

In the digital age, where disruptions and instability can impact large segments of the population at once, such failures erode the idea of continuity and regularity of public services, which is essential to administrative law. As a result, inadequate electronic service delivery could lead to administrative compensation claims based on a facility's known or assumed liability. One prominent legal example is when administration platforms have shoddy authentication procedures that permit unwanted access or fail to adequately warn users about possible data dangers. In certain situations, the public administration could be held accountable for carelessness or poor management, particularly if these mistakes cause direct injury to people. Poor performance in electronic public administration is further exemplified by operational flaws, such as failing to implement security protocols, failing to provide electronic warnings about information security risks, providing unclear instructions that allow unauthorized access, or carrying out incorrect operations that negatively impact service recipients. Legal precedents highlight the state's responsibility for these shortcomings. For example, the Supreme Court ruled in Lucknow Development Authority v. M.K. Gupta that the state must reimburse the harmed party from public funds when public employees behave in a way that is unfair to them. Both conventional and electronic methods of providing public services are covered by this principle.

- Slowness or Delay of the Public Facility:

If the administration takes longer than the reasonable amount of time required by the nature of the work to complete its tasks, this is regarded as a public service error, and the administrative body is responsible if the person is harmed as a result. It is important to remember that if the law specifies a day on which the administrative body

[1] Ibid, P. 145.

[2] Cane, Op, Cit, P. 211.

must provide its services and the body does not operate on that date, it is a sign that the administrative body has chosen not to provide its services. This indicates that although the law did not place a deadline on the administration, it did prohibit it from operating too slowly, which could have harmed people and necessitated compensation. This indicates that although the law did not place a deadline on the administration, it did prohibit it from operating too slowly, which could have harmed people and necessitated compensation.

3.2. Assumed Error:

In some cases, liability may develop based on presumed error even in the absence of a proved fault. Liability in administrative law does not always necessitate explicit evidence of fault. Faute présumée, or presumed error, is a threshold that falls in between severe liability and proven fault. In technically complicated domains like electronic public administration, where culpability and causation may be hard to establish, it enables courts to presume negligence when an administrative act causes injury. For instance, the state may be held accountable without specific evidence of negligence if a recently implemented government software system causes widespread service disruptions, such as preventing access to unemployment benefits or public health services, on the grounds that such a breakdown would not typically occur without some sort of mismanagement[1]. The administration must next demonstrate that it took all required safety measures and that circumstances outside of its control caused the harm in order to disprove this assumption[2]. This legal concept is especially pertinent in e-governance settings, where it can be challenging to pinpoint fault due to algorithmic opacity and system complexity. As a result, presumed error turns into a safeguarding legal mechanism that makes sure people aren't left without compensation only because technical evidence isn't available or is hidden by proprietary technology.

Presumptive fault has long been acknowledged by the French Conseil d'État in public liability issues involving administrative services or faulty infrastructure, and it is applied when the administration neglects to maintain crucial public systems[3]. Several legal systems have modified this theory to meet the dangers of digitization, particularly with regard to the processing of public data and the automation of service delivery[4]. In this sense, the presumption of fault is consistent with both new international governance norms, such those established by the OECD, which highlight the precautionary obligation of public administrations running digital infrastructure, and constitutional notions of administrative responsibility[5]. In electronic public administration, where technological complexity might result in unanticipated problems, this strategy is especially pertinent. For instance, even in the absence of concrete proof of fault, the administration may be assumed to have behaved negligently if a public institution implements a new software system that unintentionally results in extensive service interruptions. In addition to protecting beneficiaries, this presumption guarantees that the administration upholds strict care standards in its digital activities.

This theory permits, under some circumstances, the assigning of blame to public authorities in the context of electronic public utilities, even in the lack of concrete proof of misconduct. This strategy seeks to recompense victims and guarantee accountability, but it also presents serious practical and legal issues. The theory of supposed error, for instance, was created by the Conseil d'État, France's highest administrative court, to handle situations in which the damage is exceptional, hard to explain scientifically, and out of proportion to the anticipated result[6].

[1] Cane, Op, Cit, P. 178.

[2] Waline, Op, Cit, P. 512.

[3] Conseil d'État, Commune de Saint-Priest-la-Plaine, France, CE, 21 June 1946, Rec. Lebon 163.

[4] Tavares da Silva, Suzana, Presumed Fault and State Responsibility in E-Administrative Failures, In Administrative Law for the 21st Century, Cham: Springer, 2024, PP. 91- 105.

[5] OECD, Digital Government Review of Slovenia: Leading the Digital Transformation of the Public Sector, OECD Publishing, Paris, 2022.

[6] Duncan Fairgrieve and François Lichère. France. In Liability of Public Authorities in Comparative Perspective, edited by Duncan Fairgrieve and François Lichère, Cambridge University Press, Cambridge, 2017.

Similar to the French strategy, the UK's no-fault compensation policy in some public services aims to minimize litigation and expedite compensation procedures.

This presumption is based on the idea that, even in cases when a fault is not directly identified, the circumstances surrounding the damage strongly imply one. However, in order to apply supposed error, several requirements must be met:

- Definite Damage and Causal Link: There must be unmistakable proof of damage and a believable link between the damage and the operation of the public facility.
- Highly Likely Error: Even if an error cannot be detected with certainty, the facts should strongly imply that it occurred.
- Serious and Disproportionate Damage: The harm must be substantial and disproportionate to what was anticipated from the rendered service.

Even in cases when there is no concrete proof of culpability, this approach guarantees compensation for anyone harmed by public services. Additionally, it encourages public officials to uphold high standards of service delivery because they are aware that failure to do so may result in implied culpability. Critics counter that presumed error unfairly places the burden of proof on public authority, which could result in unfair liability. Once more, it can be difficult to determine whether supposed mistake applies, particularly when it comes to electronic public facilities where technological problems can have multiple facets. Furthermore, the use of presumed error may result in more lawsuits against public officials, which would raise questions about how best to allocate resources and the possibility of defensive tactics that could degrade the quality of services.

In order to improve adaptability and responsiveness, administrative judges are given considerable latitude in the application of French administrative law. The varied nature of administrative actions and the unique circumstances of each case may not be addressed by a strict application of the law. There are two sides to the discretion given to administrative judges when using the presumption of error. It offers the adaptability required to handle the particulars of every situation, but it also brings with it difficulties with predictability and consistency. For example, the concept of legal certainty can be undermined by excessive judicial discretion, which can result in conflicting verdicts[1]. When judges are given a lot of discretion in deciding whether the presumption of error applies, same instances may have different results depending on the judicial interpretation of each judge. This fluctuation can undermine public confidence in the legal system and make it difficult for public officials to predict potential legal repercussions. Nonetheless, this can be lessened by using the proportionality principle, which can serve as a check on the arbitrary use of discretion. Judges are therefore influenced by this principle when rendering decisions that strike a balance between the rights of public authority and the purposes of justice. This promotes justice and accountability by guaranteeing that discretion is used within appropriate limitations[2]. Judicial monitoring is essential in situations involving intricate administrative procedures, including those pertaining to electronic public services. The complexities of technical considerations can make a simple defect assessment impossible. In these situations, the presumption of error enables courts to assign blame in a way that takes into account the intricacies of the administrative procedure, guaranteeing that people are not denied redress because of the technicality of the problem.

The concept of "presumed error" permits the attribution of liability even in the absence of concrete proof of wrongdoing by transferring the burden of proof to the public authority. This concept, for instance, requires the administration to prove the absence of culpability or the involvement of an outside cause in situations when there is

[1] Jean Massot, The Powers and Duties of the French Administrative Law Judge, In Comparative Administrative Law, edited by Susan Rose-Ackerman, Peter L. Lindseth, and Blake Emerson, Edward Elgar Publishing, Cheltenham, 2017, PP. 435- 445.

[2] Jerzy Parchomiuk Abuse of Discretionary Powers in Administrative Law, Evolution of the Judicial Review Models, from "Administrative Morality" to the Principle of Proportionality, Vol. 26, Issue. 3, 2018, P. 453.

insufficient direct proof of fault. This makes it easier to compensate the harmed party[1]. However, it could be claimed that by placing an unwarranted evidential burden on public authority, the presumption of error compromises legal certainty. The burden of proof rests with the claimant, according to traditional legal norms. Deviation from this standard could result in unforeseen consequences and possible administrative liability overreach. Furthermore, it can be realistically difficult for the administration to prove blame or external causation, particularly when handling intricate administrative actions. The distinction between strict liability and fault-based liability is thus muddled by the presumption of error. Therefore, in order to resolve the issues raised by this concept, judicial review and possible legislative improvements would be crucial.

Through the use of the phrase "The damage reveals a defective performance of the public facility that naturally leads to the establishment of administrative responsibility," the Conseil d'État and lower administrative courts have indirectly or implicitly indicated the principle of "presumed error". This implies that damage inevitably signifies a malfunction in the operation of the public institution, proving the administration's responsibility. The phrase changed over time to: "The damage reveals an error in the organization or management of the facility that naturally leads to..." This change suggests a clearer mention of managerial or organizational mistakes as the foundation for culpability. The courts highlight the obligation of public bodies to uphold high standards in the administration and execution of public services by imposing liability based on assumed faults in these areas[2].

Because consumers usually interact with electronic public services remotely, without direct monitoring of the underlying systems, pinpointing the exact cause of the issue becomes extremely difficult. Therefore, users can encounter problems like access issues, data discrepancies, or system malfunctions. Users frequently lack the knowledge and resources necessary to look into and determine the precise nature of the issue due to the technological complexity involved. Users might be unfairly denied compensation in the absence of the presumption of error since they would be unable to produce comprehensive proof of the error. The French Conseil d'État granted permission to apply the "presumed error" principle to the field of electronic public utilities in the landmark Savelli case (hospital-acquired diseases) in 1960[3]. The provisions of civil liability for the custodian of the item (responsabilité du fait des choses), which impose obligation on individuals in charge of things that need special care, have therefore been claimed by certain legal scholars to be applied similarly to electronic public infrastructures. In this case, the judiciary upholds the concept of access to justice by transferring the burden of proof to the public authority, ensuring that users are not penalized for events beyond their control. As long as the damage is obvious and the circumstances point to a management or organizational failure at the facility, it should be verified that supposed fault is linked to the electronic public facilities[4].

3.3. Liability Without Fault:

Liability without negligence has become a key concept in contemporary administrative jurisprudence, especially when it comes to public service endeavors requiring intricate technology systems. Administrative accountability has historically required fault, either through an established error or an assumption of one. The state may be held accountable for damages brought on by its actions even in the absence of culpability, according to recent legal developments, which show a substantial shift toward objective liability. In the digital age, when electronic public administration necessitates the deployment of complex digital infrastructures that may unintentionally inflict harm, the idea of no-fault liability—also known as responsabilité sans faute in French administrative law—is particularly

[1] R. Widdershoven, French State Liability Law – from Path Dependency to Europeanisation?, British Association of Comparative Law, 2023, P. 25.

[2] G. Della Cananea, National and European Dimensions of French Administrative Law, British Association of Comparative Law, May 2023, PP. 1-5.

[3] Vincent Rivollier, Medical compensation under French law: fault, no-fault, and the point of liability, Otago Law Review, Vol. 16, 2019, P. 179.

[4] Jean-Victor Maublanc, Digitization of Procedures: The French Supreme Administrative Court Establishes a Presumption of Malfunction of the Public Purchaser's Dematerialization Platform Due to Difficulties in Downloading the Tenderer's Offer, Concurrences, September 2021, PP. 195–198.

pertinent. For example, even though the administration had taken adequate precautions and had not engaged in any particular act of negligence, the impacted individuals may be entitled to compensation if a cyberattack compromises the data systems of a public facility, jeopardizing personal information or service continuity[1]. In its historic decision in Natsionalna agentsia za prihodite (C-340/21), the European Court of Justice (ECJ) reaffirmed this idea, holding that the General Data Protection Regulation (GDPR) may consider the mere fear of personal data misuse after a cyber incident to be non-material damage, triggering the state's duty to compensate[2].

To further ensure that victims are not overburdened with proving technical fault, legal scholars have argued that the threshold for administrative liability should be changed in cases involving high-risk digital operations, such as biometric data processing, AI-driven public decision-making, and nationwide databases. These opinions are consistent with the public law precautionary principle, which requires administrative entities to foresee risks and pay for any consequent losses as part of their duties to the public.

In situations involving abnormal and exceptional risks (le risque spécial et anormal), including those posed by governmental technological efforts, nations like France and Egypt recognize no-fault responsibility under comparative law[3]. These frameworks guarantee fair treatment of citizens impacted by state-initiated digital transitions and are both morally and legally required. Therefore, whether by creating new cases in this area or by codifying the accepted judicial principles in the area of culpability without error, the legislature was instrumental in promoting this duty. Furthermore, unlike responsibility based on error, which necessitates the presence of the three traditional elements—the error, the damage, and the causal relationship—responsibility in this context is established once two fundamental elements are present: the damage or harm and the causal relationship between it and the administration's lawful activity. Regarding "harm," the judiciary of the French State Council demands extraordinary circumstances in order for the element of injury to establish culpability without fault; the harm in this context must be unique and exceptional. While uncommon harm indicates that it is of a certain level of seriousness that makes it unusual, specificity indicates that the harm is intended at a specific individual or at individuals themselves. Therefore, the judiciary established administrative accountability without fault for electronic public services based on the concept of risks and the equality of persons before public obligations. In certain legal systems, the phrase “risk liability” is used interchangeably with “liability without fault”.

3.3.1. No Liability for Errors Based on Risk:

The idea of risk responsibility (responsabilité pour risque) has become a fundamental component of liability without fault in contemporary administrative jurisprudence, especially in the French legal tradition. This idea, which has its roots in a practical and ethical justification, illustrates a shift away from a system that places blame and toward one that prioritizes the fair allocation of damages resulting from public actions. The fundamental idea of risk theory is that, independent of any demonstrated wrongdoing or carelessness, the person who generates a risk and gains from it must also take responsibility for its manifestation. This idea has been crucial in determining state accountability, particularly in situations when harm results from the inherent risks of legitimate official action rather than from illicit activity.

This approach has long been accepted by French administrative courts, especially the Conseil d'État, which has used it in a number of crucial areas. Notably, in cases involving dangerous products, public works projects, medical facility operations, and state-run operations requiring high-risk procedures, jurisprudence has acknowledged accountability without fault. In these situations, the administration is held accountable for exposing people to abnormal dangers in the name of the public good, not for making a mistake.

[1] Cane, Op, Cit, P. 189.

[2] European Court of Justice, Case C-340/21, Natsionalna agentsia za prihodite, ECLI:EU:C:2023:994, 14 December 2023.

[3] Nadia Yas Al-Bayati and Mohamed Najm, The Legal Basis of Administrative Liability for Damage: An Analytical Study in the French Judiciary, Journal of Legal and Political Studies, Al-Miʿyār, Vol. 8, Issue. 8, 2020, PP. 4– 12.

The French approach to travaux publics (public works), where liability is incurred not because of proved negligence but rather because people experience particular or excessive injury as a result of otherwise legal infrastructure projects, demonstrates this conceptual movement. This strategy is best shown by the landmark Cormier decision, where the Conseil d'État upheld the possibility of compensation for harm caused by public works even in the absence of administrative misconduct[1].

Similar to this, the state's role in public hospitals has come to be seen more and more through the prism of risk. Courts have acknowledged that exposure to institutional risks alone is sufficient to establish responsibility in circumstances where patients are injured due to hospital-acquired infections or defective medical equipment. The fundamental justification is distributive justice, which is focused on the fair distribution of harm brought about by collective services, rather than corrective justice, which is based on blame[2].

When it comes to risky items and techniques used by public authority, such as firearms, explosives, or hazardous chemicals, the risk theory is further applied. Even when handled properly, these objects provide an inherent risk that, if acknowledged, places the onus of harm on the government. This application focuses more on recognizing that individuals who oversee dangerous tools in the service of the public must also pay for any injuries caused by such tools than it does on penalizing mistakes[3].

Furthermore, the acceptance of risk liability demonstrates a deeper philosophical commitment: the state must serve as a last-resort insurer since it is the main actor in society. A solidaristic view of public law, in which the state not only controls risk but also bears it on behalf of its people, is reflected in this dedication. This approach changes administrative law from a strict system of fault-based responsibility into a more compassionate, socially responsive framework, as noted by René Chapus[4].

By enforcing the no-error liability principle, the French legal system upholds a core tenet of public law: that the individual should not bear an excessive burden of public service. This strategy strikes a nuanced compromise between the demands of justice and administrative effectiveness. Public institutions are now more vulnerable to new types of harm, such as hacking, cyber espionage, and data breaches, as a result of our increasing reliance on digital infrastructure. Even though these actions are usually carried out by outside parties, they can seriously harm public infrastructure and services by causing disruptions, exposing private information, and undermining public confidence. The idea of responsabilité sans faute finds additional significance in the context of these changing challenges, especially when it comes to risk liability.

- Hacking is the deliberate infiltration into electronic systems in all of its forms. This could involve using malicious code to exploit software flaws, altering transmission protocols, or gaining unauthorized access to private information. Economic espionage, political sabotage, or data theft are the goals in some situations. Such attacks, in whatever form, are directed at the digital governance infrastructure itself.
- Electronic danger also includes espionage and the following unapproved release of private information. This includes the disclosure of material that was meant to be kept private and was retained by the state or a particular institution. Whether it concerns national security, citizen personal information, or the workings of state institutions, the public revelation of such data can have just as detrimental an impact as physical assaults on public infrastructure or risky behaviors.

A workable approach for dealing with these problems is provided by French administrative jurisprudence, which is based on the principle of risk. Similar to how courts have imposed culpability for damages resulting from the

[1] Conseil d'État, 2ème et 7ème sous-sections réunies, 26/11/2012, 354108, Publié au recueil Lebon.

[2] Jean Rivero and Jean Waline, Droit administratif, 20th ed, Dalloz, Paris, 2022, PP. 812–814.

[3] Pierre Delvolvé, La responsabilité sans faute de l'administration, Revue française de droit administrative, Vol. 25, Issue. 2, 2020, PP. 230–240.

[4] René Chapus, Droit administratif général, 15th ed, Montchrestien, Paris, 2001, P. 1032.

handling of dangerous goods or faulty public infrastructure, they can also apply this principle to the issue of digital vulnerability. The same legal reasoning applies in this case: the state bears the obligation for managing the risks involved when it gains from the digitization of public services and electronic governance. Like physical infrastructure, cyber infrastructure is inherently vulnerable to damage. The disproportionate expense of such exposure should not fall on the people or organizations impacted by cyberattacks, especially when those assaults target public services. So, whether a person suffers a privacy violation, financial loss, or reputational harm as a result of a breach of state systems, this qualifies as an anomalous and unique suffering warranting reparation. In this regard, hacking and data leaks that impact public electronic facilities ought to be handled in the same way as tangible harm brought on by institutional carelessness or public works projects. The state's duty to provide compensation should be triggered by the mere exposure to anomalous risk emanating from public digital infrastructure, regardless of whether the attacker is recognized or stays anonymous, and even if the breach happens without any internal misbehavior.

Though scholars and certain judicial trends support applying risk liability to digital infrastructure, particularly when public systems are compromised and citizens suffer specific harms, it should be noted that liability without fault has not yet been fully codified in French law for cyber incidents. According to German law, a public authority cannot be held liable unless they breach a public obligation and cause harm to a third party[1]. It is more difficult to establish liability without error because this typically needs fault (purpose or negligence). Nonetheless, compensation might be provided in specific situations, such as when essential infrastructure is not secured or when the data protection law's obligation to protect personal data (DSGVO/GDPR) is broken. Regarding stringent or risk-based culpability for cyber incidents, there is still a gap. The idea of sovereign immunity, which states that the federal or state governments cannot be sued unless they agree through law, has a significant influence on the U.S. legal system. Although there are several exclusions permitted by the Federal Tort Claims Act (FTCA), cyber incidents are not specifically covered. Courts have historically been hesitant to impose culpability without explicit statutory permission or proof of egregious conduct, notwithstanding recent litigation that has attempted to hold the government accountable for data breaches, particularly those involving federal agencies (such as the 2015 OPM hack)[2]. Although there have been few remedies, the government's obligation to protect data may give rise to constitutional privacy concerns. Lastly, in the UK, people can file claims under data protection laws (particularly the Data Protection Act 2018 that implements GDPR) or negligence laws. Claims for cyber events involving data owned by the government usually involve a proven loss and a breach of duty of care. Although courts frequently set a high bar for liability, there have been several attempts at class action following significant data breaches involving public bodies (such as the NHS). Claims may also be based on the Human Rights Act of 1998, particularly Article 8 (right to private life), although there are again few remedies available unless there is evidence of serious harm.

Many nations place a high priority on cybersecurity as a governmental function for national security, occasionally limiting liability to prevent impeding defense operations. Legal systems may need to create doctrines akin to risk liability or no-fault compensation in physical infrastructure law as cyber dangers change. In this sense, the French risk theory offers a viable foundation for this kind of development, pointing the way for other common law and civil law jurisdictions to modify their legal systems to accommodate the digital era. Therefore, when based on the notion of risk, the logic of responsabilité sans faute offers a moral and legal basis for expanding state accountability into the digital realm. It is consistent with a more comprehensive view of public law, where the state guarantees justice in the face of modern technology threats in addition to acting as a regulator and protector.

3.3.2. Equality Before Public Burdens: No Error Liability

The two primary grounds for liability without fault recognized by French administrative law are equality before public burdens, which emphasizes that legitimate administrative action shouldn't cause disproportionate harm to individuals or groups, and risk theory, which highlights the existence of abnormal danger or technical hazard. Both

[1] Helmut Koziol and Barbara C. Steininger, European Tort Law, Springer, Vienna, 2008, PP. 137–138.

[2] In re Office of Personnel Management Data Security Breach Litigation, 928 F.3d 42, D.C. Cir. 2019.

frameworks uphold the notion that state liability is redistributive as well as corrective, acknowledging that justice in public administration must take into consideration both individual loss and group gain. One of the fundamental tenets of individual liberties and rights is the equality of people before burdens. Everybody must pay these taxes and public expenses when they are imposed by the state; no one may avoid them or have them placed on them. Even when there is no unique risk involved but harm is an unavoidable and disproportionate result of activities committed for the public benefit, this argument warrants culpability based on distributive fairness. This principle states that the state must make sure that no one person or small group is disproportionately affected negatively by measures it takes that serve the public good. If such harm takes place, compensation becomes an obligation based on equity and fairness rather than merely an administrative choice. This equality-based obligation addresses routine administrative actions that, while legal and generally advantageous, result in specific, direct, and unique harm to certain people. In this case, the harm or injury is a predictable and essential byproduct of the state's pursuit of the general welfare[1] rather than an incidental or unusual one. In this case, the harm results from the unequal distribution of the responsibilities that public policies invariably create rather than from a breakdown in public service or a duty violation. Therefore, the law requires the state to restore equality through compensation even in the absence of danger or administrative error. This was made abundantly evident in the landmark case of Couitéas, when the principle of equality before burdens dictated that compensation was due for the substantial and individualized injury caused by the unwillingness to expel squatters from private land, even though it was legally authorized in the purpose of maintaining public order[2].

The reasoning is simple: it is unfair for only a select few to experience the negative externalities of public policies if they are intended to benefit society as a whole. The state must acknowledge that the collective benefit must be matched by an equal allocation of expenses, for instance, when infrastructure investments result in expropriation, interruption, or financial loss to particular persons. Furthermore, this type of liability is especially pertinent in modern fields like cybersecurity, urban planning, and environmental regulation, where the harm is frequently caused by necessary and extensive administrative activity rather than dangerous practices. In the digital age, the same reasoning holds true: if the government digitizes its services for efficiency and the good of the country and a specific citizen is harmed by a systemic failure or data compromise, compensation ought to be provided—not due to risk or fault, but rather because an imbalance in burden has arisen[3].

The principle of equality before public services (égalité des usagers devant le service public), which states that all people in the same legal situation should have equal access to public services regardless of personal characteristics like wealth, location, or background, is one of the fundamental promises of e-administration. Theoretically, e - administration upholds this idea by providing services continuously and remotely and by eliminating geographical and temporal constraints. In actuality, though, digital inequality adds a new level of prejudice that jeopardizes the fundamental ideal that e-administration is supposed to support. Even if the statutory requirements for using public digital services are implemented consistently, some groups may be de facto excluded due to structural and technological inequalities, such as unequal access to devices, internet connectivity, and digital literacy. Even though they are legally entitled to e-services, people who are elderly, economically disadvantaged, or lack digital literacy may find it difficult or impossible to use them[4].

Furthermore, public digital services might only be accessible in specific regions or might be tailored for particular hardware or operating systems, resulting in an unequal environment where equal rights are not accompanied by equal capabilities. Therefore, even while the law acknowledges that all individuals are equal before the public service, the way eadministration is designed and implemented may result in unfair treatment and unintentionally limit access to privileged groups—those who have the requisite technical resources and expertise. These

[1] Chapus, Op, Cit, PP. 1042- 1046.

[2] Conseil d'État, Couitéas, 30 November 1923, Rec. Lebon, P. 789.

[3] Frédéric Rolin, L'égalité devant les charges publiques à l'ère du numérique, Revue française de droit administratif, Vol. 35, Issue. 3, 2019, PP. 510–519.

[4] Mireille Delmas-Marty, Libertés et droits fondamentaux, Seuil, Paris, 2020, PP. 232–234.

discrepancies go against the fundamental administrative law tenet that all users must have nondiscriminatory access to public services. Scholars of French administrative law have pointed out that formal legal equality is only as significant as material equality in service access. When the state decides to digitize vital services, it also takes on the responsibility of making sure that everyone can use them, including through universal service design, targeted assistance for vulnerable customers, and supplementary analog channels[1].

The French Conseil d'État has long maintained that, particularly in cases where new modalities are implemented, access to public services must be tailored to the requirements and abilities of users. The logic of equality before public burdens and public services would imply that any public service transformation, digital or otherwise, must take into account and mitigate systemic disadvantages that prevent equal enjoyment of public rights, even though comprehensive jurisprudence in the field of e-administration is still lacking. Therefore, eadministration runs the risk of going against the fundamental tenet of treating all users equally when it replaces traditional service routes without guaranteeing inclusive access. In these situations, structural exclusion—a failure to design systems that fulfill the universal accessibility inherent in public service obligations—may give rise to administrative culpability rather than technological malfunction or negligence.

3.3.3. Refusing Liability For Errors:

By proving that there was no negligence or error on the part of the public authority that caused the damage, the authority can disprove this assumption of error. This can be accomplished by proving that an outside factor—such as the injured party's activities, the actions of a third party, or force majeure—caused the damage and was beyond the authority's control[2]. The public authority might not be held accountable, for example, if a user unintentionally caused the damage by their own conduct or if an unforeseen circumstance resulted in the damage. Liability is therefore not absolute in the absence of fault. General principles of causation still apply to it. Notably, the administration can be absolved of all or part of its culpability by claiming the existence of a foreign cause (cause étrangère), which is an outside factor that breaks the causal link between the administrative action and the harm. In this context, foreign causes are grouped based on how they affect the legal attribution of liability[3]. Whether or not the administration is held liable, there are several circumstances that totally absolve them. These include the victim's act (le fait de la victime), which occurs when the harmed party is accountable for their own injury due to careless or deliberate behavior, and force majeure (la force majeure), which is an unpredictable, unavoidable, and external event.

However, other causes—like a third party's mistake or a fortuitous event (le fait d'un tiers or cas fortuit)—usually only result in exoneration in cases involving guilt; they do not stop culpability without fault, especially when it comes to the theories of risk or equality before public duties[4].

For electronic public facilities, this divergence has important ramifications. Since many of these services are digital and run continually, there is a significant chance that outside threats, technical malfunctions, or third parties will interfere. However, unless they satisfy the strict requirements of a foreign cause that can sever the causative link91, these do not always absolve the administration of culpability[5]. For example, the administration can successfully reject responsibility in the framework of culpability without fault only under the following situations:

[1] Jean Waline, L'égalité des usagers devant le service public à l'ère du numérique, Revue française de droit administratif, Vol. 36, Issue. 2, 2020, PP. 215-225.

[2] Vincent Rivollier, Medical compensation under French law: fault, no-fault, and the point of liability, OtaLawRw 10; 2019, 16 Otago LR , P. 179.

[3] Pierre Delvolvé, Responsabilité de l'administration et cause étrangère, Revue française de droit administratif, Vol. 17, Issue. 2, 2001, PP. 235-243.

[4] Frédéric Rolin, Cyberadministration et responsabilité: la force majeure est-elle encore invocable?, Les Petites Affiches, Issue. 150, 2020, PP. 12-18.

[5] Frédéric Rolin, L'administration numérique et la responsabilité sans faute: vers une nouvelle catégorie de risques?, Revue française de droit administratif, Vol. 38, Issue. 2, 2022, PP. 210-219.

- The disruption of underwater internet connections due to a force majeure event, like a deep-sea earthquake, could cause administrative websites or services to go offline. Unpredictability, irresistibility, and exteriority in relation to the administration's sphere of influence are characteristics of such an event.
- The victim's action, such as when a citizen willfully creates a system error that causes their self-injury, carelessly enters inaccurate data, or abuses the digital platform[1].

However, in situations of liability without fault, factors like a third party's mistake (for example, a hacker breaching the public platform's security infrastructure) or an unexpected technical issue (for example, a virus interfering with public servers) typically aren't enough to break the chain of causation[2]. In the context of contemporary digital administration, these causes are not unexpected even though they are outside the administration's control. Courts are likely to take into account the administration's obligation to foresee and protect against such risks, particularly when handling critical public services, given the recognized incidence of cyber-attacks. In this perspective, a cyberattack does not represent a force majeure event; rather, it is a typical aspect of digital risk that the administration needs to understand and protect against[3].

Conclusion:

The study highlights that digital technical failures are no longer merely technical glitches, but have become a real source of administrative accountability, especially in an environment increasingly dependent on digital systems for public service delivery. The results showed that the administration bears a significant portion of the responsibility for these failures, whether the error is proven or not, as long as the damage occurred and could have been avoided through preventative measures and sound management. It also demonstrated that the absence of effective technical planning and weak digital governance increase the likelihood of system failures and undermine customer confidence in public services. Therefore, achieving a balance between digital modernization and the administration's legal liability is essential to ensuring service sustainability and efficient performance.

The legal approach revealed that determining the administration's liability for digital technical failures is linked to the degree of error and the possibility of proving it. The administration remains responsible whenever it is proven to have failed to take measures to prevent the failure or mitigate its effects. In cases where it is difficult for the injured party to prove the error, accountability for the administration is justified based on the presumption of presumed error, especially when the failures are recurrent or result from a clear oversight weakness. In cases involving vital facilities or essential services that cannot be interrupted, the administration may be held liable even in the absence of fault, based solely on the theory of harm. This reflects an evolution in legal thought toward protecting digital rights and compensating for associated damages. This trend reinforces the need for the administration to adopt proactive policies and secure technologies to limit liability and enhance public confidence in the digital system.

Acknowledgement

The author would like to express sincere gratitude to the University of Abderrahmane Mira – Béjaia, Faculty of Law and Political Sciences, for providing the academic environment and resources necessary to conduct this research. Special appreciation is extended to colleagues and fellow researchers who provided valuable feedback and constructive insights during the preparation of this study.

Conflict of Interest

[1] Jean-Bernard Auby, Le droit de l'administration numérique, Dalloz, Paris, 2021, PP. 103–105.

[2] European Court of Human Rights, López Ribalda v. Spain, App. No. 1874/13, judgment of 17 October 2019.

[3] Mireille Hildebrandt, Algorithmic Accountability in Public Administration: A Legal Perspective, Artificial Intelligence and Law, Vol. 28, Issue. 4, 2020, PP. 403–420.

The author declares no known financial or personal conflicts of interest that could have influenced the research, analysis, or conclusions presented in this paper.

References

1. Bloomberg, J. (2018). Digitization and digital transformation: Confuse them at your peril (p. 6). Forbes.
2. Katz, R., & Koutroumpis, P. (2012). Measuring socio-economic digitization: A paradigm shift (p. 35). Columbia Institute for Tele-Information.
3. Ruiz, M., & Soto, A. (2013). National digital strategy. National Digital Strategy Coordinator.
4. Tang, C., & Perumal, R. M. (2013). The characteristics and values of e-governance and the role of e-democracy. International Journal of Humanities and Management Science, 1(1), 142.
5. Singh, A. (2023). E-governance: Moving towards digital governance. Vidya: A Journal of Gujarat University, 2(1), 204–215.
6. OECD. (2020). The OECD digital government policy framework: Six dimensions of a digital government. OECD Publishing. https://doi.org/10.1787/4de9f5bb-en
7. Charalabidis, Y., Flak, L., & Pereira, G. (2022). Scientific foundations of digital governance and transformation: Concepts, approaches and challenges. Springer.
8. Jopang, J., Aryatama, S., Muazzinah, M., & Qamal, Q. (2024). Exploring the relationship between e-government, transparency, and citizen trust in government services. Global International Journal of Innovative Research, 2(6), 1354–1363.
9. Bora, I., Duan, H. K., Vasarhelyi, M. A., Zhang, C., & Dai, J. (2021). The transformation of government accountability and reporting. Journal of Emerging Technologies in Accounting, 18(2), 1–21. https://doi.org/10.2308/jeta-19-005
10. Ibrahimy, M. M., Norta, A., & Normak, P. (2023). Blockchain-based governance models supporting corruption-transparency: A systematic literature review. Blockchain Research and Applications, 5(2), 1–21.
11. Nabben, K., & De Filippi, P. (2024). Accountability protocols? On-chain dynamics in blockchain governance. Internet Policy Review, 13(4), 1–22.
12. Straub, V. J., Hashem, Y., Bright, J., Bhagwanani, S., Morgan, D., Francis, J., Esnaashari, S., & Margetts, H. (2024). AI for bureaucratic productivity: Measuring the potential of AI to help automate 143 million UK government transactions (pp. 1–18).
13. Deloitte. (n.d.). AI: Can smart technologies drive government efficiency? Retrieved from https://www.deloitte.com/us/en/Industries/government-public/articles/ai-in-federal-government.html
14. Djatmiko, G. H., Sinaga, O., & Pawirosumarto, S. (2025). Digital transformation and social inclusion in public services: A qualitative analysis of e-government adoption for marginalized communities in sustainable governance. Sustainability, 17(7), 3–4.
15. Chary, M. (2011). Social equity, the digital divide and e-governance: An analysis of e-governance initiatives in India (p. 65). University of South Florida.
16. Kolotouchkina, O., Barroso, C. L., & Sanchez, J. L. M. (2022). Smart cities, the digital divide and people with disabilities. Cities, 123, 1–4.
17. OECD. (2024). Enabling digital innovation in government: The OECD GovTech policy framework. OECD Publishing.
18. Al-Ansi, A. M., Garad, A., Jaboob, M., & Al-Ansi, A. (2024). Elevating e-government: Unleashing the power of AI and IoT for enhanced public services. Heliyon, 10, 10–11.
19. Janssen, M., Hartog, M., Matheus, R., Ding, A. Y., & Kuk, G. (2022). Will algorithms blind people? The effect of explainable AI and decision-makers' experience on AI supported decision-making in government. Social Science Computer Review, 40(2), 478–493.