Volume 2 Issue No. 12 December 2025

QGS Group
Delivering excellence since 1993

Quality Herald

The voice of excellence

THE EVOLUTION OF DIGITAL IDENTITY RIGHTS

OWNERSHIP, PRIVACY & CONTROL IN THE NEW DIGITAL FRONTIER

Table of Contents

ABOUT THE JOURNAL

*The **December 2025** edition of **Quality Herald** spotlights the theme **"The Evolution of Digital Rights"**, exploring how global societies are redefining privacy, data ownership, and digital freedom in an increasingly connected world. This edition delves into the shifting landscape of rights in the digital era, shaped by rapid technological advancements, regulatory transformations, and rising citizen awareness.*

Through in-depth features, expert analyses, and exclusive interviews, this issue examines how governments, tech companies, and civil society are navigating the complexities of digital identity, surveillance, cybersecurity, and AI governance. It highlights the growing need to balance innovation with protection, ensuring that individuals retain control over their digital footprints while still benefiting from the opportunities created by emerging technologies.

By unpacking these critical developments, the December edition provides readers with valuable insights into the future of digital citizenship and the global push for ethical, transparent, and inclusive digital ecosystems. It offers a compelling perspective on how the evolution of digital rights is shaping policy, business practices, and everyday life - empowering individuals and guiding societies toward a more secure and equitable digital future.

Title	Quality Herald – The Voice of Excellence
ISSN	
Language	English
Frequency of Publication	Monthly
Starting Year	2023
Format of Publication	Online
Publisher	Quality Growth Services Private Limited (QGS Group)
Publisher Address	H-13, Kirti Nagar, New Delhi – 110015, India
Contact Numbers	+91-11-25431737 / 25918332 / 41425273
Emails	qgs@qgspl.com / info@qgspl.com
Website	www.qgspl.co.in
Editor-in-Chief	Dr. Sumit Shandilya (sumit@qgspl.com)
Managing Editor	Sachin Grover (sachin@qgspl.com)
Associate Editor	Surajit Mukhopadhyay

Aims	The magazine intends to be leading platform for sharing practical insights, innovative ideas and thought leadership in the field of Quality, Sustainability, Operations and Business Excellence. It seeks to inspire professionals, academicians and organisations to adopt and implement the quality driven approaches that leas continuous improvement and societal value.
Scope	A. Management System B. Sustainability and ESG practices C. Operational and Business Excellence D. Women empowerment E. Youth, Education and Future of Quality Leadership F. Industry 4.0 and Artificial Intelligence
Submission Email	info@qgspl.com
Review Policy	All articles will be reviewed for relevance, clarity, and adherence to guidelines. The editorial board may conduct a light review or seek peer feedback where required. Feedback and decision (acceptance, revision, or rejection) will be communicated within 1–2 weeks.
Plagiarism Policy	Strictly zero-tolerance. All submissions must be original and appropriately cited.
Availability	Available online on the publisher's website.
Author Guidelines	Submission Format • Title of the Article • Full Name(s) of Author(s) • Affiliation(s) and Designation(s) • Contact Email(s) • Author Bio (50–100 words) • Declaration of Originality • Main Content (with headings/subheadings) • Conclusion / Key Insights • References • Tables/Figures (if applicable – clearly labeled) Word Count Guidelines 1. Feature Articles / Case Studies: 1500–3000 words 2. Opinion / Technical Notes: 800–1500 words 3. Book Reviews / Interviews / Brief Insights: 500–1000 words 4. Longer manuscripts may be considered based on editorial merit. Formatting Instructions 1. Font: Calibri or Times New Roman, Size 11 or 12 2. Line spacing: 1.15 3. Use clear sub -headings and bullet points 4. All visuals must be referenced in-text 5. No plagiarism and provide appropriate citations

Quality Herald – The Voice of Excellence
Vol-2, Issue-12 | December 2025

As we arrive at the final issue of Volume 2, I am reminded of how quickly the landscape around us continues to evolve and how essential it is for us, as professionals and lifelong learners, to stay one step ahead of the curve. December is always a moment of reflection, gratitude and forward thinking. It is also an opportunity to close a year with clarity and begin the next with purpose.

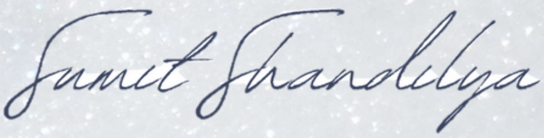
Our theme for this edition is ***The Evolution of Digital Identity Rights,*** *a topic that has moved from theoretical discussion to everyday reality within a remarkably short span of time. Digital identity is no longer limited to passwords, biometrics or access control. It has become a fundamental expression of individual rights, privacy, security, ownership and trust in a world that is now shaped by data.*
From the rapid rise of AI generated content to the increasing adoption of decentralized identity frameworks, the question is no longer whether digital identity will influence our lives. The question is how prepared we are to navigate this shift responsibly and intelligently. Organizations today are redefining quality, governance and customer trust through stronger authentication systems, transparent data policies and user centric digital ecosystems. Individuals are becoming more aware of how their identity is captured, stored, interpreted and used.

In this issue, our industry practitioners and academicians bring deep insights on the legal, ethical and technological evolution of digital rights. You will also find our regular features, including thought provoking essays, industry news, case insights, the ever popular crossword section and reflective commentaries on how organizations across sectors are responding to this new frontier.

Quality Herald has grown steadily this year because of the unwavering support of our readers, contributors and well-wishers. To every author who shared expertise, to every reader who wrote back with thoughts and suggestions, and to every professional who continues to believe in the power of knowledge, I extend my sincere appreciation.

As we prepare for the next volume, I warmly invite you to share your articles, experiences, opinions and ideas with us. Your voice adds richness and diversity to this community and helps us stay grounded in real world perspectives.

Thank you for being with us through this journey.
Wishing you a meaningful end to 2025 and a promising start to the year ahead.



Chief Editor
Quality Herald – The Voice of Excellence

Editorial Board

Contact us:
Phone: +91-11-25431737 / 25918332, Email: qgs@qgspl.com / info@qgspl.com

Published by
Quality Growth Services Private Limited (QGS Group)
H-13, Kirti Nagar, New Delhi – 110015 India

Digital Identity Rights: Navigating the New Frontier of Privacy, Security, and Empowerment

Article from the Editor's Desk - Surajit Mukhopadhyay

In the digital age, where much of our personal lives are increasingly conducted online, the concept of digital identity has become a cornerstone of modern society. From social media profiles to online banking, digital identities govern how individuals interact with the virtual world. However, with this growing integration of technology into daily life comes a critical concern: digital identity rights. The evaluation of these rights is more urgent than ever, as they touch on issues of privacy, security, freedom, and even human dignity in a space that often operates without borders.

What Is Digital Identity?

A digital identity is essentially a collection of data and attributes that represent an individual or entity in the digital world. It can include basic identifiers like names and email addresses, biometric data, digital certificates, online behaviour patterns, and even social media activity. All of this information shapes how a person is recognized, authenticated, and authorized in online spaces.

As the world becomes increasingly digital, the need for secure and verified digital identities has never been more pressing. However, with the advantages of digital identities come significant risks, including data breaches, identity theft, and surveillance. This is where the evaluation of digital identity rights comes into play — it is the process of assessing and ensuring that these identities are not only protected but also respected in a way that promotes fairness, autonomy, and privacy.

Why Digital Identity Rights Matter

Digital identity rights refer to the rights individuals have over their own personal data in the context of their online presence. These rights are integral to ensuring that people have control over how their data is used, who can access it, and for what purpose. The following points highlight why these rights matter:

- Privacy Protection: With vast amounts of personal data circulating online, individuals are increasingly vulnerable to privacy violations. Ensuring that people have the right to control their digital identities can help protect them from unwanted surveillance or misuse of personal information.
- Security: Digital identities are often targeted by cybercriminals for fraud, theft, and other malicious activities. A strong framework for digital identity rights can help establish security protocols that safeguard individuals' information and prevent unauthorized access.
- Autonomy and Freedom: Individuals should have the right to define how they wish to present themselves online, without coercion or manipulation. Without proper protections, people could face forced or unwanted exposure, such as in cases of online harassment, data scraping, or algorithmic bias.
- Access and Inclusion: A growing number of government services, financial institutions, and healthcare systems require digital identities for access. Ensuring the fairness and inclusivity of these systems is critical for avoiding discrimination and ensuring equal opportunities for everyone, regardless of socioeconomic status or technological literacy.
- Accountability and Transparency: As more private companies collect and store individuals' data, there is an increasing need for accountability in how digital identities are managed. Digital identity rights help ensure that individuals can demand transparency from organizations handling their personal information and hold them accountable for any misuse.

Key Issues in the Evaluation of Digital Identity Rights

As governments, tech companies, and civil society grapple with the concept of digital identity rights, several key issues emerge that complicate the evaluation process.

- Data Ownership and Control: One of the most contentious issues in digital identity rights is the question of who owns an individual's data. Many users are unaware that their personal information is being collected, stored, and sold by companies. Digital identity rights must address whether individuals have the right to own, control, and erase their data, or if this power rests with the corporations that collect it.
- Interoperability vs. Fragmentation: While digital identity systems are being developed to streamline access to services, they are often fragmented across platforms and jurisdictions. For example, a digital ID issued by one country might not be recognized in another. Similarly, private sector systems (such as Google or Facebook accounts) might not communicate with government-based identity systems. Balancing the need for interoperability with the protection of individual rights remains a significant challenge.
- Government Surveillance and Data Privacy: Governments around the world are exploring the use of digital identities for everything from e-voting to public health initiatives. However, the centralized nature of government-managed digital IDs raises concerns about surveillance and the potential for authoritarian control. Evaluating digital identity rights requires addressing the balance between facilitating services and protecting citizens from overreach.
- Biometric Data and Consent: With biometric systems — such as facial recognition and fingerprint scanning becoming increasingly common, the use of sensitive data for identity verification has raised important ethical questions. Who owns biometric data? How can we ensure that this data is not misused? And how can people withdraw consent if they no longer wish to participate in these systems? These questions need clear, universally accepted guidelines to protect individual privacy.
- Algorithmic Bias and Discrimination: Digital identity systems can be prone to biases, especially when algorithms that determine access or validation processes are not properly tested for fairness. Racial, gender, or socio-economic biases embedded in digital identity systems can lead to discrimination in areas such as job recruitment, credit scoring, and access to services. Ensuring that these systems are designed and implemented with fairness and transparency is crucial for upholding digital identity rights.

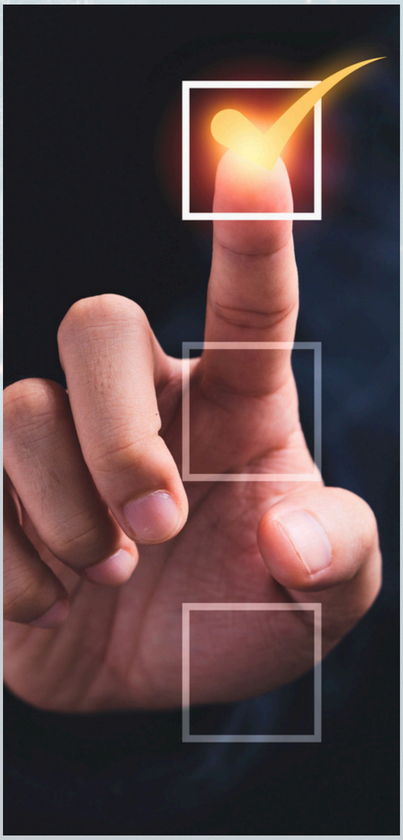
The Role of International Standards and Regulations

As digital identity systems expand globally, the need for international frameworks and standards becomes even more critical. Several regions have already started to implement or propose regulations that aim to protect digital identity rights:

The European Union's General Data Protection Regulation (GDPR) sets out stringent rules around data protection and privacy. The GDPR gives individuals significant rights over their personal data, including the right to access, correct, and delete their data. While not focused exclusively on digital identity, it lays an important foundation for the evaluation of digital identity rights in the EU.

The United Nations has also weighed in on the importance of digital identity, recognizing it as a fundamental human right. The UN's “Universal Declaration of Human Rights” can be interpreted to include the right to digital identity, particularly in the context of access to services, freedom of expression, and the right to privacy.

The OECD (Organisation for Economic Co-operation and Development) has developed guidelines for the protection of privacy and the governance of digital identities. These guidelines aim to ensure that digital identity systems are used in a way that respects human rights and fosters trust in digital ecosystems.



Moving Forward: Ensuring Fairness and Protection

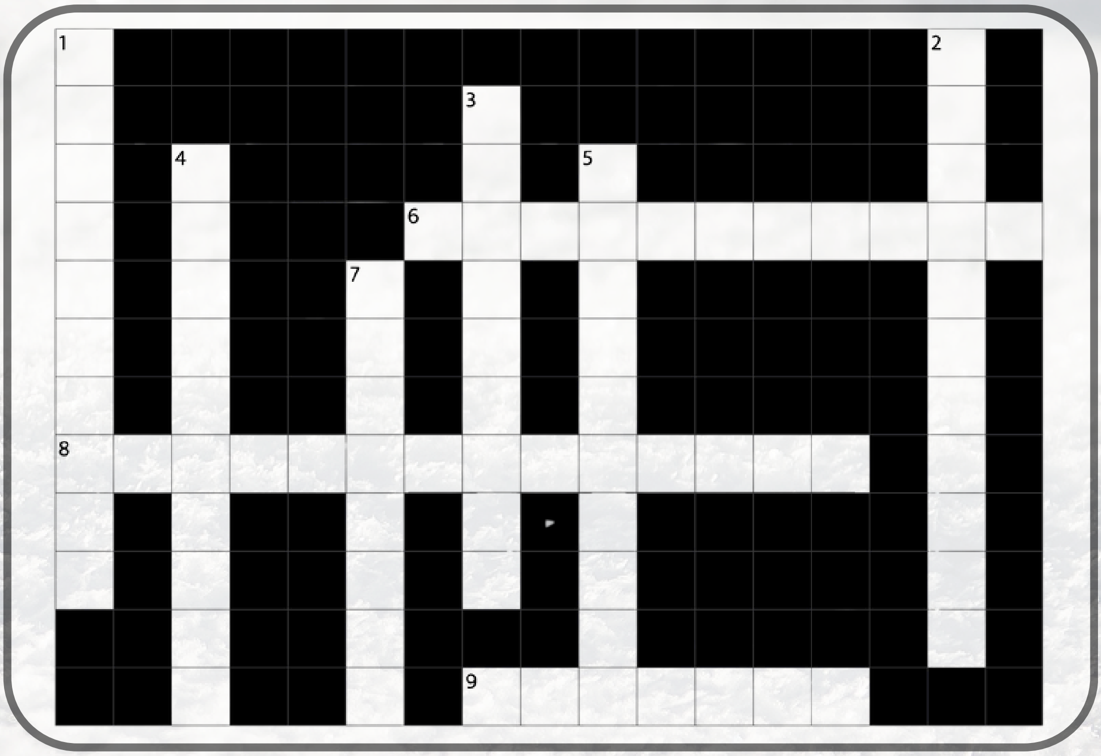
The evaluation of digital identity rights is an ongoing, complex process that will likely evolve as technology continues to advance. Moving forward, it is essential for governments, tech companies, and civil society to work together to develop clear, robust, and adaptable frameworks that ensure digital identity systems are secure, transparent, and equitable.

The rise of decentralized identity models, such as self-sovereign identity (SSI) systems, offers a potential solution to some of the challenges related to data ownership and control. These systems aim to give individuals full control over their digital identity without relying on centralized entities.

In the end, the evaluation of digital identity rights must not only be about protecting individuals' data but also about respecting their autonomy and dignity in an increasingly connected world. By addressing issues such as security, privacy, consent, and fairness, we can ensure that digital identity systems serve as tools for empowerment rather than oppression, facilitating greater participation in society and securing human rights for all.

The evaluation of digital identity rights is a pressing issue that touches on fundamental principles of privacy, freedom, and security in the digital era. As digital identities become more central to how we live, work, and interact, it is crucial that we establish systems that protect individuals' rights while fostering innovation and inclusion. With thoughtful regulation, ethical design, and a focus on fairness, we can navigate the complexities of digital identity and build a safer, more equitable digital future.

IDENTITY RIGHTS CROSSWORD

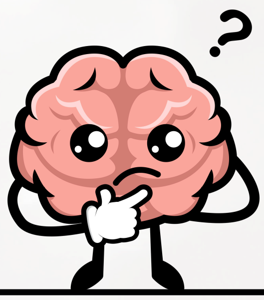


ACROSS

6. Distributed ledger tech often proposed for secure identity systems.

8. Process that verifies a user's identity (passwords, tokens, biometrics).

9. Unique physical or behavioral traits used to identify a person.



DOWN

1. State of being unidentifiable within a set of users.

2. Permission given by an individual for collection or use of their data.

3. Principle that individuals (or nations) control identity data about themselves.

4. Laws and rules that govern how digital identity data is used.

5. The ability to move your identity data across services.

7. The right to control who accesses your personal information.

10. The set of attributes that uniquely represent a person in digital systems.

Answers of the Previous edition

Across: 1.Resilience, 3.Ceo 7.Entrepreneurship 8.Strategy 9.Influence 10.Vision

Down: 2.Empowerment, 4.Leadership, 5.Governance, 6.Innovation

A New Era in Labour Governance

Sachin Grover - Managing Editor, QGS

India's labour laws have undergone a historic transformation in November 2025, with 29 fragmented legislations consolidated into four modern labour codes. These changes reshape wages, social security, workplace safety, and industrial relations, impacting both employees and employers across sectors.

India's labour framework, long criticized for being outdated and complex, has been streamlined into four comprehensive labour codes:

Code on Wages, 2019 – Establishes a national minimum wage, standardizes the definition of wages, ensures timely payment, and enforces equal pay for equal work.

Key Highlights

• Uniform Definition of Wages - A standard definition across all labour laws ensures clarity in salary structures, allowances, and benefits.

• Mandatory Minimum Wages - Applies to all workers in both organised and unorganised sectors, ensuring no one is left behind.

• Timely Payment of Wages - Employers must pay wages on time, whether daily, weekly, or monthly, reducing disputes and delays.

• Equal Remuneration - Reinforces the principle of equal pay for equal work, regardless of gender.

• Bonus Provisions - Workers earning below a certain threshold are entitled to statutory bonuses, strengthening income security.

Industrial Relations Code, 2020 – Modernizes rules for trade unions, hiring and retrenchment, dispute resolution, and industrial peace.

Key Highlights

• One Code, Many Laws - Consolidates three major legislations — the Trade Unions Act (1926), Industrial Employment (Standing Orders) Act (1946), and Industrial Disputes Act (1947) — into a single, streamlined framework.

• Empowered Trade Unions - Recognition of unions is now formalised. A union with majority membership (51%) becomes the sole negotiating body, ensuring stronger collective bargaining.

• Flexibility with Fixed-Term Employment - Employers can hire workers for fixed terms, but with equal benefits as permanent staff — including gratuity eligibility.

• Strikes & Lockouts Under Control - Mandatory 14-day notice before strikes or lockouts across all sectors, reducing sudden disruptions and fostering dialogue.

• Retrenchment & Closure Thresholds Raised - Companies with up to 300 workers can retrench or close without prior government approval, giving businesses more operational flexibility.

Social Security Code, 2020 – Extends benefits like gratuity, provident fund, and insurance to gig workers, platform workers, and media professionals, ensuring wider coverage.

Key Highlights

Consolidation of Laws - Merges nine social security legislations (like EPF Act, ESI Act, Maternity Benefit Act, etc.) into a single code for simplicity.

Universal Coverage - Extends EPFO and ESIC benefits nationwide, bringing more establishments and workers under mandatory social security.

Gig & Platform Workers Recognised - For the first time, gig and platform workers are formally recognised. A Social Security Fund is created for their welfare.

Maternity & Women-Centric Provisions

- 26 weeks of maternity leave.
- Mandatory crèche facilities in certain establishments.
- Option for work-from-home arrangements for women.

Gratuity Reform - Fixed-term employees become eligible for gratuity after just one year of service (earlier five years), benefiting contract/project workers.

Appointment Letters & Minimum Wages - Mandatory appointment letters and guaranteed minimum wages for all workers, including informal and gig workers.

Digital Compliance & Ease of Doing Business

- Technology-driven "Inspector-cum-Facilitator" system.
- Digital records and filings.
- Decriminalisation and compounding of minor offences.

Social Security for 400 million Workers - The code aims to cover over 40 crore workers across India, including those in informal sectors.

Occupational Safety, Health and Working Conditions Code, 2020 – Enhances workplace safety standards, regulates working hours, mandates appointment letters, and strengthens protections for women and contract labour.

Key Highlights

Consolidation of Laws - Replaces 13 central labour laws (covering factories, mines, plantations, contract labour, inter-state migrants, etc.) with a single code, reducing multiplicity and overlap.

Uniform Standards Across Sectors - Establishes common rules for occupational safety, health, and working conditions across industries, states, and union territories.

Registration & Licensing Simplified - Introduces a single registration system for establishments and a common licence for contractors, easing compliance burdens.

Working Hours & Leave

- Maximum daily working hours capped at 8 hours.
- Mandatory annual leave with wages for workers.
- Clear provisions for overtime compensation.

Health & Welfare Provisions -

- Mandatory health check-ups and safety measures.
- Provision of drinking water, sanitation, canteens, first-aid, and crèches in larger establishments.
- Focus on women workers' safety, including night-shift provisions with safeguards.

Inter-State Migrant Workers

- Enhanced protections and portability of benefits.
- Mandatory registration of migrant workers for access to welfare schemes.

Technology-Driven Inspection - Inspector-cum-Facilitator system introduced for transparency, using digital tools to reduce harassment and improve compliance monitoring.

Employer Obligations - Employers must provide a safe working environment, free from hazards, and ensure welfare facilities are accessible to all employees.

Labour Code – Key focus & Action Points

Short Term Focussed	Medium Term Focussed	Long Term Focussed
Review payroll and the new definition of Wages	HR Policies overhaul	Compliance Governance model
Understand and implement the “working hours”& “Overtime rules”	Standing Orders readiness	Align documentation & contracts
Verify contractor compliance on timelines, wages, overtime & records	Systems & HR management system updates	Workforce strategy realignment

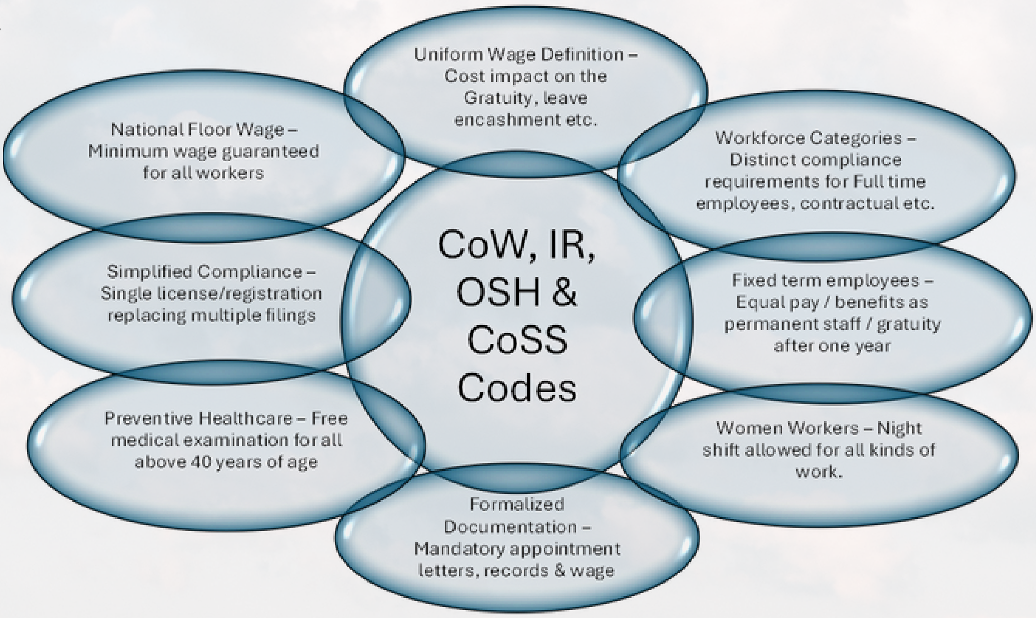
Key Changes Employees Should Know

- Universal Minimum Wage: A national floor wage ensures fair pay across states.
- Mandatory Appointment Letters: Every employee must receive a formal letter of appointment, reducing informal employment practices.
- Social Security Expansion: Gig workers, contract labour, and even media professionals are now entitled to benefits like insurance and provident fund.
- Gratuity Access: Workers can access gratuity benefits more easily, even in fixed-term employment.
- Working Hours & Leave: Clear regulations on maximum working hours, paid leave entitlements, and overtime compensation.
- Women’s Rights: Enhanced provisions for women, including night-shift employment with safety measures.
- Simplified Compliance: Digital record-keeping and reduced paperwork for employers, balancing ease of business with worker protection.

Balancing Worker Rights and Business Flexibility

While the codes strengthen employee protections, they also streamline compliance for industries. For instance:

- Employers benefit from uniform definitions of wages, reducing disputes.
- Layoff thresholds have been revised, allowing businesses more flexibility in workforce management.
- Trade unions gain clearer recognition processes, but dispute resolution mechanisms are designed to minimize prolonged conflicts.



Quality Growth Services Pvt. Ltd.

Your partners in excellence

Established in 1994, Quality Growth Services Pvt. Ltd. (QGSPL) is a leading consultancy firm specializing in Quality, Environmental, and Safety Management Systems. With a mission to foster a culture of quality and continuous improvement, QGSPL collaborates with expert consultants trained by premier European institutions. We empower organizations to enhance efficiency, achieve compliance, and improve profitability.

Our offerings include world-class training and consultancy services, including Lead Auditor certification, management awareness programs, and internal audit workshops tailored for global industries.

Our Core Services

▶ ***Training Programs***

Customized training solutions on management systems, internal auditing, statistical tools, and decision-making techniques, designed specifically for senior and mid-level professionals.

▶ ***Ecoservices***

End-to-end sustainability solutions focused on decarbonization, ESG compliance, resource optimization, and green transition strategies—enabling organizations to build a sustainable future.

▶ ***Management System Consulting***

Expert guidance in implementing, auditing, and achieving certification for ISO standards such as:

- ***ISO 9001 (Quality Management)***
- ***ISO 14001 (Environmental Management)***
- ***ISO 45001 (Occupational Health & Safety)***

qgs@qgspl.com | info@qgspl.com +91 1125431737 / 25 | +91 98332 41425 / 273

The Digital Identity Rights Evolution.

Kumar Sarthak - Audit Assistant , JM Associates

Identity has been and always been a determinant of how people interact in the society even though in the recent years it has begun to take a new digital shades. The ration or voter ID required to form identity, in the contemporary day, identity goes as far as biometrics databases, mobile applications, social media profiles as well as algorithmic assessments being conducted in the background. As the world and India shift more and more toward digitally mediated systems, one might be curious about how identity is changing and what sorts of rights will be able to be invoked in order to secure individuals in this changed setting.

Widening Digital Identity.

The digital identity is no longer limited to certain personal information that is registered in the government offices. It has now incorporated biometric markers, Internet behaviour, monetary conduct, web browsing, location tracking and conclusions drawn by companies and algorithms about individuals. It gives the example of India, where its own Aadhaar ecosystem has provided more than 1.33 billion people in India with a distinctive biometric identity, becoming one of the largest digital identity systems in the world.

Other than Aadhaar, digital identity is also becoming applicable in other areas. The existence of mobile KYC transactions, UPI-based transactions, Documents in Digi Locker, and facial recognition in the airports show the level of ubiquitousness of digital identity verification in life. Such systems are handy, but they also raise certain questions in terms of privacy, independence and future use of information- some of the questions that can be useful to consider prior to usage.

Digital Identity Short history.

History of the Internet: Anonymous and the early years.

The first internet encouraged low self-disclosure and pseudonymies. The communication was done by use of usernames and there was little correspondence between offline and online identities. This air gave freedom, but it was not very serious about the digital rights or the data protection.

The Movement to Reality Identity and Social Media.

During 2005-2015, the social networks began linking the online activity to the real world identities. Pictures and destinations, crowds and details about oneself were typical. Facebook and WhatsApp in India became a part of everyday communication, which provokes more and more concerns about the disclosure of information and fake news. Meanwhile, financial inclusion and authentication services and welfare delivery were simplified on Aadhaar-linked systems.

This period of time increased the salience of the digital identity, and this demonstrated gaps in comprehending how data were stored, analysed or shared, behind the scenes.

Biometrics, Artificial Intelligence and Predictive Identity: The Age of Biometrics.

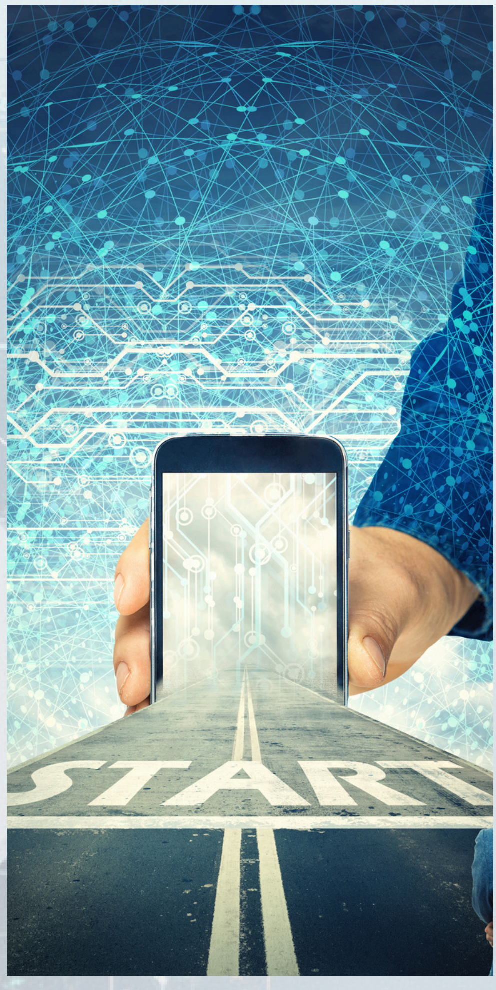
Over the past few years, the digital identity is on a different level that is characterized by biometrics and artificial intelligence. Facial recognition is being tested in the DigiYatra programme by Indian airports. Banks entail voice and face authentication. Behavioural profiles are used by E-commerce services and credit bureaus, and the fintech businesses are increasingly reliant on AI-based risk modelling.

As identity is increasingly becoming more interrelated and information-intensive, fairness, transparency and inclusion are legitimate concerns. The potential opportunities are enormous, so are the threats, such as deepfaked identities to identity theft, data leakage and potential automated discrimination in decision systems.

The importance of Reflecting on Digital Identity Rights in the Present day.

The Privacy Is becoming more complicated.

Users often leave personal information in applications, services and systems and most of them do not know the extent of discontinuation of information. In India the Digital Personal Data Protection Act (DPDP) that came into law in 2023 attempts to augment the rights of the users on consent and data minimisation. Despite the fact that it is still on its implementation phase, it is a sign that more glaring safeguards may be needed as digital identity systems expand.



Risks of Exclusion Remain

Welfare and payments are accessible to millions of people via digital identity systems, and it can also be misused to criminalise individuals who lack access to reliable internet, smartphones, or even updated documents. The cases of authentication failure in Aadhaar-based systems applied in public distributions, despite the fact that the number dropped down during the past couple of years, make one ponder how identity systems can be made more accommodating and resilient.

Rising Security Concerns

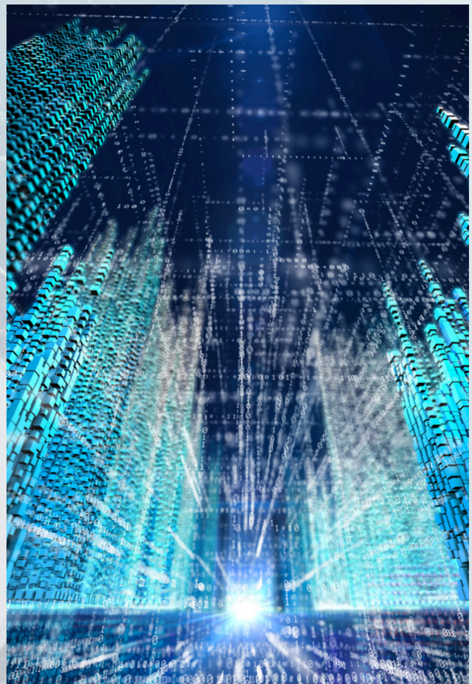
It is a result of the high use of digital payments that the number of identity fraud in India increased significantly. The instances of sim card abuse, UPI frauds, biometric cloned-based frauds indicate that there is a higher possibility of implementing additional protective mechanisms. Since it can be done through deepfakes to form a highly believable impersonation, nowadays, fraud is not limited to stolen passwords, however, stolen face and voice are also possible.

Information and Decision-Making Focus.

Big systems of identity are massive, as in the case of Aadhaar, DigiLocker or KYC databases constructed by the private sector, which crunch mass amounts of personal data. It might be beneficial to some that people should have more access to the manner in which their data are held and used or that decentralised solutions can be safer.

Problems that are to be discussed continuously.

- Despite frameworks like the DPDP Act beginning to put a mark over the data practices, there are also several areas that can receive a more thorough consideration:
- Consent is a complex issue. It is known that human beings will accept things without reading or knowing. Basic and more significant consent directions could be useful.
- The users can appreciate systems that allow them to know or challenge automated results when the Opaque means of access to credit or jobs are automated.
- The practices of data sharing are ambiguous: Access to identity data by third parties - no matter fintech, e-commerce, or advertising- can be made more transparent.
- Laws are not the same in all industries: there are industries strictly covered with regulations compared to others. A better-coordinated stand would contribute to reducing confusion.
- Biometric dependence is two-way Biometrics are convenient and unlike passwords, they cannot be altered in case of compromise.



Future Trends

Decentralised Identity with More User Control: Self-Sovereign Identity (SSI) models may offer alternatives to centralised databases in which individuals can store and share their credentials on the selective basis. Research on these models would help in identifying whether they can be used in India with its size and diversity.

Unexpected Transparency in AI decisions: India might also enjoy a more even-handed understanding of the explainability and fairness policies as AI expands into lending, insurance, staffing, and service delivery to the public. Users can be empowered provided they could explore the basis of autonomous judgments concerning their identity.

rivacy as an intrinsic system architecture: Privately designed systems, a system where privacy is considered and designed as opposed to an after-thought can alleviate threats. Such practices are also encouraged by the DPDP Act through data minimisation encouraged in India by the DPDP Act that could guide the future identity systems.

Interoperability and Inclusion: India is equally developing rapidly in the sphere of interoperable digital services, Aadhaar, UPI, or even Digi Locker. Incorporation of these systems especially to rural and low-income people may be more important than technological creativity.

SATISFY
EXCEL WITH STANDARDS

SATISFY India – Driving Excellence Through Standards

For more than 30 years, SATISFY India has been the trusted ally for organizations looking to stay ahead in a rapidly evolving business landscape. We connect you to the right national and international standards - helping you stay compliant, competitive, and future-ready.

Standards We Provide: AIAG | ISO | ASTM | IEC | BIS | IEEE | BS | AAMI

Why SATISFY India?

- **30+ years of trust and reliability**
- **End-to-end compliance and lifecycle management**
- **Access to the world's most recognized standards**
- **A partner that ensures your business is always ahead of the curve**

What We Offer

- **Global Standards Access – Seamless availability of international benchmarks.**
- **CSUM Standard Monitoring – Stay updated with the latest changes.**
- **Tailored Compliance Solutions – Designed to fit your business needs.**
- **Industry Expertise – Insights built on decades of knowledge.**
- **Customized Approach – Because one-size never fits all.**
- **Lifecycle Support – From adoption to implementation and beyond.**

Partner with SATISFY India—and navigate today's complex regulatory environment with ease and confidence.

www.satisfyindia.com ***info@satisfyindia.com***

Reinventing Identity: The Rise of Digital Rights in a Connected World

Yerra Anudeep Chowdary - Sales Executive, BlueStone

The concept of identity has experienced one of the most tremendous changes in the history of humankind in the past 20 years. What existed physically previously, in the form of passports, IDs, signatures, face to face interaction, has now rolled out into a sophisticated digital layer that marks the way people operate in the contemporary world. Digital identity is not only an extension of our identity today it is a key that opens us to economic systems, social communities and governance by the people. With the expansion of our digital presence, the issue on the rights, ownership, privacy, and control over this identity is now emergent among the 21st century parameters.

Physical Identity to Digital Presence.

An identity, since ages, has been pegged on material objects. An individual could establish his identity through demonstration of physical documents which were given by credible authorities. This model was not altered much till the emergence of the internet. As communication, business, and institutions moved to the digital platform, the old mechanism of verifying identity grew insufficient. The first generation of digital identities (email address, online usernames, login passwords) dates back to the early 2000s. Such platforms as Google, Facebook, and Amazon became identity providers by default. The same login was used to access various services, and it made it simpler to use and have a centralized control to the private corporations. This period was the start of a new dilemma, despite the convenience, the users were not the owners of their digital identity; corporations were.

The Era of Surveillance Capitalism

With the growth of digital contacts, the quantity of personal data gathered by corporations grew as well. Each click, search, ping of location and each on-line purchase added to an increasing digital biography. Megabuildings realized the potential of this data in the economy and developed business cycles based on focused advertising and behavior profiling. This gave rise to so-called surveillance capitalism a system in which businesses gather, process, and sell information about their users with or without their knowledge or disclosure. Digital identity was not just a log in credential; it was now a commodity. The extent of data gathered and the level to which their activity on the internet could be profiled was not made known to the users. The absence of strict regulations at this time enabled firms to be very irresponsible. There was virtual absence of digital identity rights and people were not much in control of how their identity is used or represented in the Internet.

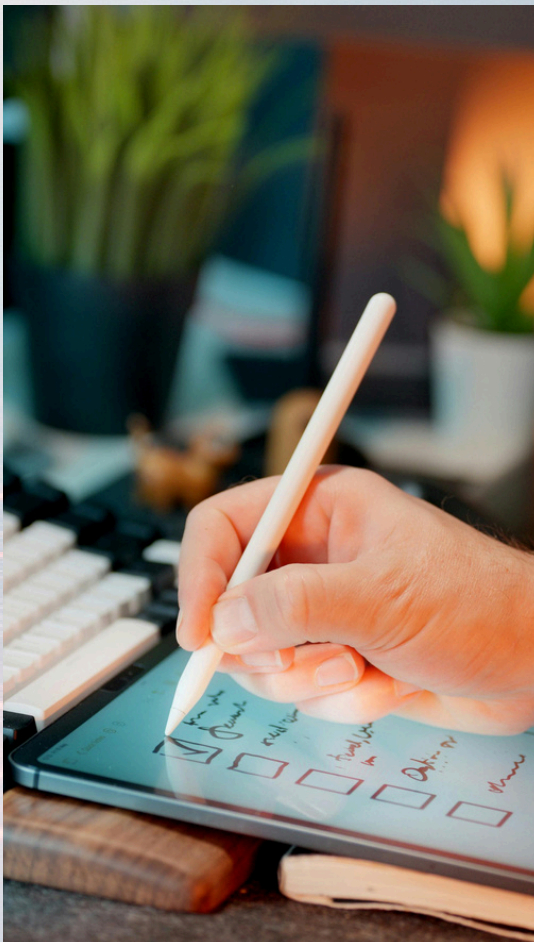
Awakening to Privacy and Control

This was a turning point as the information breaches, misinformation campaigns, and privacy invasion started getting noticed around the world. The unauthorized data mining and manipulation has been revealed on high-profile events and people have become hyper-conscious of the security risks associated with their online identities. The reaction of the governments and civil society organizations was to lobby stronger data protection laws. Such concepts as the right to be forgotten, data portability, and informed consent became part of the public opinion. The rights to digital identities ceased to be an abstract concept but became a legal requirement

Government-Led Digital Identity Systems

Since digital interactions are now part and parcel of life, with the advent of digital interactions, numerous governments have established digital identity systems to allow access to government services in a secure way. The introduction of systems such as the Aadhaar system in India, the eID program in the EU, and digital driver's licensing in various countries was an indication of transitioning to state-controlled digital identity. These systems were going to be efficient- there was going to be quick access to welfare schemes, easier checking, and less fraud. Nevertheless, they also expressed their concerns regarding surveillance, centralization, and abuse of biometric data. The development of the digital identity rights during this stage focused on the establishment of a balance between:

- Convenience and privacy
- Security and freedom
- State good and personal freedom.



Rise of User-Owned Digital Identity

A major shift began with advancements in cryptography and decentralized technologies. Blockchain-based digital identity systems introduced a new paradigm: self-sovereign identity (SSI). In this model, individuals own, store, and control their personal data, sharing only what is necessary, and only with explicit consent.

SSI frameworks propose a world where:

- A person can prove their age without revealing their date of birth.
- They can verify their address without sharing the entire document.
- They can login to services without creating multiple usernames or handing over unnecessary data.

This marks a radical rethinking of digital identity rights—moving from platform-controlled identity to user-controlled identity. Instead of being passive data sources, individuals become active participants who own and manage their digital identities.

Conclusion

The development of digital identity rights has been a measure of how far we've come through digitisation, social changes, and the evolving need to protect our fundamental freedoms as individuals. The history of digital identity has been a continuous negotiation between power and autonomy; it has ranged from fragmented log-in credentials through the rise of surveillance capitalism to government ID programs and decentralized ownership of identity. The evolution of technology continues, so now it is up to policy makers, the tech community, and We the People to ensure that digital identity is a tool for empowerment and not for exploitation. Digital identity rights are about more than just protecting our digital information; they also encompass protecting our dignity, freedom, and individuality in today's digital world

INSTITUTE FOR INDUSTRIAL PERFORMANCE & ENGAGEMENT

औद्योगिक क्षमता एवं समावेशन संस्थान | QGS Group

Boost Your Career with IIPE India's Industry-Recognized Certification Programs

At IIPE India, we believe in empowering professionals with the knowledge, skills, and credentials that today's industries demand. Our certification programs are designed to close the gap between talent and opportunity, preparing you for growth in a competitive job market.

Our Flagship Certification Programs

- *Certified Industrial Manager – Quality (CIMQ)*
- *Certified Industrial Manager – Maintenance (CIMM)*
- *Certified Quality Lab Practitioner (CQLP)*
- *Certified Lean Engineer (CLean)*
- *Certified Lean Leader (CL²)*

Why Choose IIPE India?

✓ *Industry-Focused Curriculum – Training aligned with market needs*
✓ *Expert-Led Learning – Insights from seasoned practitioners*
✓ *Flexible Study Options – Learn at your pace, on your schedule*
✓ *Recognized Credentials – Strengthen your profile and credibility*

Take charge of your career today!
Enroll in IIPE India's certification programs and unlock new opportunities for success.

www.iipeindia.com *info@iipeindia.com*

From Documents to Data: The New Age of Digital Identity Rights

Pranjal Tripathi, RPMG – Loan portfolio Manager, Axis Bank

The world within just 30 years has radically changed its perception. Initially, a digital presence was regarded as a mere novelty. Now it is considered a vital and indispensable human identity extension. Our names, behaviors, likes, financial records, and even biometric identifiers are way out there in huge digital universes. Consequently, the idea of digital identity rights, which was once obscure and hypothetical, has now become the most urgent socio-legal issue of the 21st century.

In today's world, digital identity is far from being just a username or an online profile. It is a collection of data that essentially portrays a person's way of life in the contemporary world. Whether it is using the banking services or applying for a job, availing healthcare services or engaging in social activities, digital identity is the lifeblood of the civic world and the economy. Hence, it is not merely a technological story, but a major shift in social structures where power, independence, and even citizenship change the face of the digital era.

From Data Collection to Data Autonomy

The internet period, along with its bright days, was dark for the users' data privacy: users had little knowledge of and even less power over the way their data was collected. Usually, in digital interactions, the deal was as follows: users would get free services, while companies would collect their data. Such an unbalanced move established the first generation of digital identity which portrayed corporations as the custodians and the winners of the personal data game.

One effect after another, on-time data breaches and Big Tech platform rising led to a reevaluation of personal data's use to the world. The revelation of the Cambridge Analytica's scandal was a turning point in recognizing the use of digital identity as a tool for purposely exploiting and dominating the manipulated audience. It brought about the global realization that follows: people demand transparency, states recognize regulation requirements, and tech companies welcome the new norms of the game.

The change from data collection being a passive act to data control and management centering on users symbolizes in a large part the evolution of digital identity rights. Current regulations increasingly provide for the observance of such principles as the informed consent, limitation of use, and the rights for inspection or erasure of personal files. In essence, the line of thought is that digital identity will be a property of human beings rather than a thing which companies only use.

Digital Identity as a Human Right

Or better say, as digital identity is a prerequisite for participation in economic and civic life, it is inevitably becoming one of human rights. Initially, access to technology was regarded as a luxury but now it is the foundation of individual freedom and equal opportunities.

There is a large number of countries where people who do not have proper digital credentials are deprived of access to basic services. In such cases, Digital ID structures act as gatekeepers to welfare subsidies, healthcare, and financial sectors. Despite the benefits that these systems offer in terms of efficiency, they also spark off numerous ethical problems, for example, what happens during technology breakdowns? Who takes the blam when data mistakes lead to rights being denied? Should digital ID be seen as a basic right? Most people have slowly begun to believe that digital ID must match the values of human rights like worth, privacy, and freedom. This also covers keeping people safe from unfair acts by AI models, ensuring clear rules when choices are made by machines, and giving people the right to hide their ID whenever they want. As far as digital worlds grow, the line between a person's real and online self gets less clear, which pushes the human rights laws to change for the new truth.

The Rise of Self-Sovereign Identity

Technological innovation has also been a major factor in the transformation of digital identity. One of the most revolutionary ideas over the last years is SSI—an idea where people have the right to, and are the managers and controllers of, their own identity information, without the need for centrally governed authorities.

With the support of decentralized systems like blockchain, SSI allows the user to share information with whom they want, for example, an institution. The user, instead of a bank or a government, keeps the personal documents, which then can be verified without the need of showing more than necessary to the verifier.

For example, let's say you want to prove you are over 18 years old to somebody. Instead of giving your full birth date, you can just provide the piece of info "Age Verified" with the help of SSI methods. By doing so, the risk of overexposing the data is minimized and the power behind identity is transferred from organizations to users.

SSI is heralding a world in which digital identity will be not only legally safeguarded but inherently designed to protect privacy. It changes the face of identity from being one of the things stored in big data warehouses to an independent digital asset, which is under the control of users and not companies.

Biometrics and the New Frontier of Consent

Biometric technologies such as fingerprint scanning, facial recognition, and voice identification have become integral to digital identity, adding a new dimension to it. Unlike a password, a person's biometric characteristic cannot be replaced. This makes the data very "strong" but at the same time "risky" for the user.

One of the fastest ways to demonstrate upsides as well as setbacks of any technology is to show how it is rapidly spreading in a particular field, in this case publicly and privately. Biometrics performance-wise are great in terms of security and comfort, but worries about established surveillance, profiling, and misuse follow them closely. The ethical dilemma is clear: how societies benefit from biometric technologies without losing freedoms remains the question?

The turn to consent is vital in the story. Just agreeing to privacy terms reading without attention is not enough when one's identity is presented as the mathematical representation of their face. Thus, future digital identity rights should come with precisely defined protections for biometric data, strict usage limits, and the provision for individuals to disagree with or decline automated recognition systems.

Digital Identity and Algorithmic Justice

With more and more of the decisions—such as loan granting or hiring—that are done by algorithms, the interaction of digital identities with systems that judge, class, and label people is increasing. The justice of these systems has a direct connection with opportunities and human dignity of those affected.

Algorithmic discrimination usually results from the fact that the training data for the developers of machine learning models contains biases, hence these models inherit these biases. This means digital identity could be the root of a new kind of inequality if no regulations are held. The evolution of digital identity rights should be inclusive of the right to algorithmic transparency as well as the ability to challenge automated decisions.

Simply put, digital identity and digital justice have become inseparable. To protect the rights of digital citizens, it is also necessary to ensure that algorithms recognize them fairly and treat them equally.

The Road Ahead: Towards a Rights-Driven Digital Society

One of the main factors to shape technology, policy, and public awareness will be the future of digital identity rights. When people realize more and more the worth and the risk of their digital selves, the call for better safeguards will not stop but keep going higher.

The data-protection laws are becoming more stringent as governments are spreading the world over because of their efforts, and at the same time, technology companies are asked to implement privacy-by-design frameworks. The coming phase of the digital identity will probably entail worldwide standards for digital identity governance, borderless data-portability rules, as well as tightened regulation of digital platforms.

The most essential thing is that the story about digital identity is getting less and less about control and more and more about empowerment. The new objective goes beyond merely regulating data to allowing people to use their digital identities for further self-governance, respect, and access to more possibilities.

Conclusion

The change of digital identity rights to be a story of power given to the user, risk, and transformation. With users having very little knowledge about data collection, we are now moving toward an era where people demand control over their digital selves which is exactly what they are getting. The protection of digital identity as a matter of privacy is becoming the most important issue out of human rights as technology keeps dissolving the separation between our physical and virtual lives. Digital identity will be an important factor in determining our working, communicating, traveling, and social interacting methods in the coming years. It is necessary to keep strong digital identity rights if we want to create a just, safe, and open digital world of tomorrow.

Quality Growth Services Pvt. Ltd.
Your partners in excellence

QGS Sustainability Programs for a Greener Future

QGS is committed to advancing sustainability by helping businesses achieve carbon neutrality, net-zero emissions, and resilience against climate risks. Their expertise spans ESG, circular business models, and sustainability communication, ensuring responsible growth.

- **Net Zero Emmissions**
- **Decarbonization**
- **Carbon Neutrality**
- **Strategy for mitigation & Adaptability**
- **Business Responsibility and Sustainability Reporting (BRSR)**
- **Materiality**

Innovative solutions for sustainable living today

Together, we can create a more sustainable world for future generations to enjoy.

The New Self: Navigating the Era of Digital Identity and Data Rights

N Jithin Kumar - Business Partner, Rrayze business solutions

Walk down any busy street today and you'll see people unlocking phones with their faces, tapping to pay with digital wallets, scanning QR codes, or signing documents with a fingerprint. These scenes, once futuristic, are now everyday rituals. But behind each effortless gesture lies a profound shift in the very nature of identity—moving it from wallets and filing cabinets into the vast, abstract, and sometimes unpredictable expanse of the digital world. This new era raises an urgent question: What does it mean to own your identity in a world where your existence is increasingly online?

Welcome to the evolution of digital identity rights—the movement redefining who we are, how we prove it, and what protections we deserve in the digital age.

From Paper Trails to Digital Footprints

For centuries, identity rested in paper—birth certificates stored in home drawers, passports checked at borders, licenses presented for verification. These documents worked, at least in a world where interactions happened in person and systems moved slowly. Then came the internet.

What started as a simple username-password combination quickly evolved into sprawling digital footprints scattered across social media platforms, e-commerce accounts, government portals, and financial apps. Databases became the new gatekeepers of our identity.

But centralization came with a cost. One breach could spill millions of identities onto the dark web. One platform's poor security became everyone's problem.

This vulnerability sparked the earliest conversations about digital privacy, data protection, and the right to control one's personal information.

The Biometric Boom

By the early 2010s, biometrics burst onto the scene.

A person's face, fingerprint, voice, or iris became tools for instant verification. Airports deployed e-gates. Banks adopted fingerprint-based KYC. Smartphones began unlocking with a glance.

Biometrics promised convenience and security, but introduced a deeper philosophical question: What happens when the password… is you? Stolen passwords can be changed. Stolen biometric data cannot.

As governments and corporations embraced these technologies, the call for stronger digital identity rights grew louder.

When Identity Became Mobile

The next leap was the rise of mobile IDs and digital credentials. Nations like Estonia, India, and Singapore built ecosystems where citizens could access healthcare, banking, education, and public services through a single digital identity.

Identity was now: Portable, Ubiquitous, Always-on

With that convenience emerged new risks: data profiling, mass surveillance, and over-collection of personal information. It became increasingly clear that identity wasn't just a tool—it was a form of power. And citizens wanted that power back.

Digital Identity Rights: The New Civil Liberties

As digital identity became indispensable for participating in modern life, rights around it grew essential.

The Right to a Legal Digital Identity- The United Nations now considers identity a global developmental priority. Without a recognized digital identity, individuals risk being locked out of education, banking, healthcare, and democratic participation.

The Right to Privacy- Citizens want (and deserve) a say in how their data is collected, stored, and shared. Privacy is no longer a preference—it is a right.

The Right to Security- Digital identity systems must be protected from breaches, fraud, impersonation, and misuse. Security is the foundation upon which trust is built.

The Right to Consent and Control- The era of "click to accept" is fading. Users want transparency—and true control.

The Right to Portability- Identity shouldn't be locked within a single platform or provider. It must move with the individual, interoperable across borders and services.

The Future: Identity as a Human Right

The next decade will redefine the very architecture of identity.

Expect:

- Digital wallets holding government IDs, diplomas, financial credentials, medical records
- AI-driven identity systems that analyze behavior, not just documents
- Quantum-resistant encryption safeguarding identity assets
- Global digital identity frameworks enabling borderless participation
- Stronger human-centered policies protecting autonomy, consent, and rights
- The future of identity is not just technological—it is ethical.
- As we march deeper into a digital-first century, the question isn't whether digital identity will shape our lives. It already does. The real question is whether the systems we build will protect individuals as much as they empower institutions.

Conclusion: Defining Who We Are in a Digital World

The evolution of digital identity rights is, at its heart, the story of modern humanity. It reflects our values, our fears, our vulnerabilities, and our aspirations in a rapidly changing world.

Identity is no longer a document. It's a dynamic, living construct that travels with us across devices, platforms, and borders. And as our digital selves grow more powerful, so must the rights that govern them.

The challenge—and opportunity—before global society is clear:

Build a future where digital identity empowers individuals, protects their dignity, and strengthens their freedom.

That future isn't decades away. It's unfolding right now.

NEWS

The Digital Personal Data Protection Act, 2023: Most urgent policy intervention in India

India has officially notified the rules under the DPDP Act — making it the country's first comprehensive data-privacy law to protect digital personal data and give real rights to individuals.

The law replaces the older, outdated framework (dating to when smartphones and mass digitization didn't exist) — a legal vacuum that had left huge gaps in data security, accountability, and citizen protection even as India's internet adoption and digital services exploded.

What DPDP changes / enables

- Individuals (data-owners) now have explicit rights like consent, access, correction, erasure, and the right to revoke consent.
- Entities (data-fiduciaries) handling digital personal data, be it e-commerce, fintech, social media, healthcare, etc. are mandated to follow strict safeguards: encryption, access controls, breach notifications, audits, etc.
- A new enforcement body, Data Protection Board (DPB), is set up to handle complaints, investigations, and penalties including heavy fines (up to ₹250 crore) for serious breach or negligence.

Why this matters — and why earlier gaps were risky

Before this law:

- There were no clear, uniform rules around how much data could be collected, how long it could be stored, or who was accountable if data was misused.
- Big data leaks and breaches had exposed sensitive info — from identity numbers to health and personal records — showing that earlier frameworks were insufficient for today's scale of digital adoption.

Now with DPDP, India aims to build a more secure, rights-aware digital infrastructure — one that balances innovation with privacy, and gives individuals more control over their data.

Important Dates in December 2025

Navy Day (India) – 4 December (Thursday)

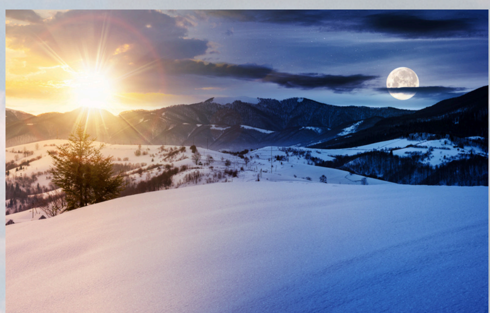
Celebrates the achievements and strength of the Indian Navy. The day honors naval heroes and recognizes their significant contribution to national security.

Human Rights Day – 10 December (Wednesday)

Marks the adoption of the Universal Declaration of Human Rights. It emphasizes global commitment to equality, dignity, and justice for all.

Milad-un-Nabi (Shia) – 12 December (Friday)

Commemorates the birth anniversary of Prophet Muhammad for Shia Muslims. The day is observed through sermons, prayers, and community gatherings.



Winter Solstice – 21 December (Sunday)

The shortest day and longest night of the year in the Northern Hemisphere. It symbolizes the transition toward increasing daylight and holds cultural significance worldwide.

New Year's Eve – 31 December (Wednesday)

The final day of the year, celebrated with enthusiasm across countries. People observe it with parties, reflections, and anticipation of new beginnings.

NEWS

Digital Personal Data Protection Rules 2025 (DPDP 2025) and concerns raised by the telecom sector

What's the news

- According to a recent report by Cellular Operators Association of India (COAI), major telecom operators in India - now designated as "significant data fiduciaries" under DPDP 2025 — say many of their concerns from public consultations remain unaddressed in the final notified rules.
- Key unresolved issues include: unclear security-compliance framework, ambiguous methods for minor age verification, rigid rules around consent-management, and potential conflict with existing sector-specific laws.

What telecom firms are worried about

- Because telecom firms already operate mature networks with security controls, they argue that applying a "one-size-fits-all" compliance approach under DPDP may be unnecessary and inefficient — suggesting a "layered, risk-based" approach instead.
- The rule that prohibits directors or key personnel of data-fiduciaries from working with "consent managers" is seen as "overly stringent." COAI proposes allowing either a unified consent-management layer for the whole telecom sector or allowing robust internal consent systems rather than forcing external consent managers.
- There's concern about overlapping regulatory requirements and duplicate breach-reporting obligations under DPDP and existing telecom/IT laws. Telecom firms want a harmonised, single reporting mechanism to avoid redundancy and confusion.

What this means more broadly

- The concerns reflect the challenge of applying new, sweeping data-protection rules to sectors like telecom, which handle huge volumes of sensitive personal data and already operate under strict regulations.
- If unresolved, these issues could lead to compliance difficulties, operational burdens, and potential legal ambiguities - affecting not just telecom operators but also end-users, regulators, and the broader digital economy.
- It also shows that while DPDP 2025 aims to strengthen individual data rights, practical realities and sector-specific contexts (like telecom) need clearer, harmonised regulation for effective implementation.


Merry
Christmas
&
Happy
New Year

QUALITY CONTROL(LED) HUMOR

When Work Gets Too Serious

1. THE COOKIE CONSENT SAGA 🍪

User: "I just want to read the article."
Website: "First accept essential cookies… then functional.. then emotional support cookies."
User: Accepts everything -"Take my data, I give up."

2. PRIVACY POLICY UPDATE #127 🔐

Company: "We've updated our privacy policy."
User: "What changed?"
Company: "Nothing you'll ever read, but it feels responsible to notify you."

3. THE AI MONITORING MOMENT 🤖

Employee: "Is the new AI tool tracking productivity?"
Manager: "No, no… it's just observing, predicting, analyzing, and documenting. Very harmless."

4. THE DATA OWNERSHIP DEBATE 📊

Customer: "Do I own my data?"
App: "Yes."
Customer: "Do you sell my data?"
App: "…Define 'sell'."

5.THE 'TERMS & CONDITIONS' LIE 📜

App: "Do you agree to the terms & conditions?"
User: clicks Agree
App: "You didn't even scroll…"
User: "Neither did you when you wrote them."

GLIMPSES

Completed a detailed EHS Internal Audit at a leading automotive ancillary firm in Gurgaon, evaluating statutory compliance, operational practices, and potential risk exposures. The audit reinforced the organization's commitment to safety, sustainability, and continuous improvement by strengthening its EHS management systems across functions.

A comprehensive 4-day workshop on Business Process Reengineering was conducted for the support services of a global tyre manufacturer, focusing on analysing current workflows and identifying improvement opportunities. The initiative aimed to streamline operations, enhance cross-functional efficiency, and strengthen service delivery excellence across the organization.

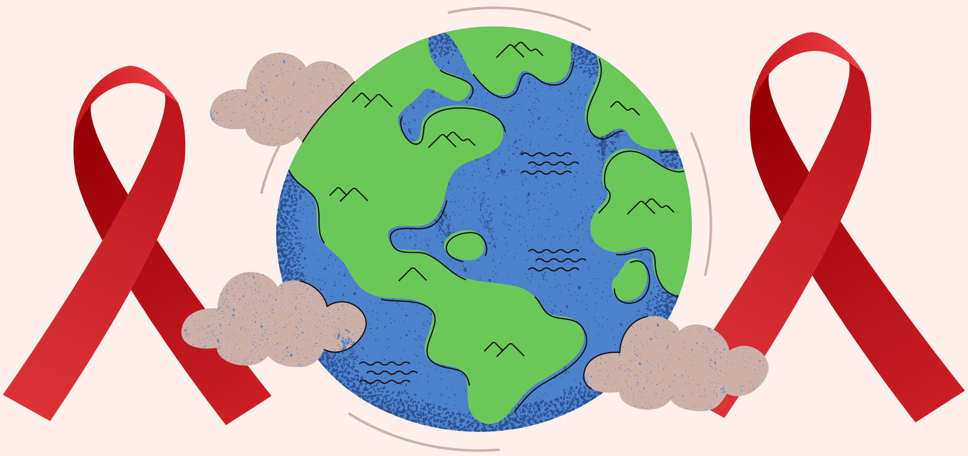
Conducted an EHS Internal Audit training program at a leading automotive ancillary unit in Pune, covering key compliance frameworks and risk-assessment techniques. The initiative enhanced audit preparedness and deepened workforce capabilities in identifying and addressing EHS gaps. It further supported the organization's commitment to building a safer, more accountable, and sustainability-driven operational culture.

Delivered an IATF training programme at a leading automotive manufacturer, focusing on key quality management system requirements and industry best practices. The initiative enhanced process discipline, compliance readiness, and operational consistency across teams. It empowered participants with practical tools for auditing, documentation, and continual improvement. The programme further reinforced the organization's commitment to world-class quality and customer satisfaction.

AIDS DAY

DECEMBER 1ST 2025

START WITH YOU TO STOP AND
REMIND EVERYONE NOW ON.



**STOP HIV TO SPREAD
BECAUSE WE CARE FOR
OUR FUTURE.**

MAKE THE PEOPLE AROUND US HEALTHY AND
HAPPY PEOPLE. NO ONE CAN BUY OUR HAPPINESS
AND HEALTH. SO TAKE GOOD CARE OF THEM.

Upcoming Training Programmes

Dec. 01-05, 2025

ISO 9001:2015 Lead Auditor

Dec. 15-19, 2025

ISO 14001:2015 Lead Auditor

Starting from Dec. 19, 2025

Lean Six Sigma Black Belt

Dec. 22-26, 2025

ISO 45001:2018 Lead Auditor

January 07-09, 2026

ISO/IEC 17021-1:2015

Contact to Register or Inquire

https://qgspl.co.in/

+91-11-25431737

Quality Growth Services Pvt. Ltd.
Your partners in excellence

"The evolution of digital rights is not about technology; it is about dignity, autonomy, and the right to be seen on our own terms."

Quality Herald: The Voice of Excellence
H-13, Kirti Nagar, New Delhi, India 110015

Phone : +91-11-25431737/25918332/41425273
Email: qgs@qgspl.com / info@qgspl.com

