Kathmandu School of Law Review (KSLR),
Volume 12, Issue 1, 2023, pp 113-125
https://doi.org/10.46985/kslr.v12i1.2225

The Need for data protection law in Nepal: Securing Citizen's Rights in the Digital Age

Dr. Newal Chaudhary[*]

Abstract

Nepal is undergoing rapid digitization of services across sectors like education, commerce, finance and healthcare. However, this digital transformation has enabled mass collection of citizens' personal data by both government and private companies without sufficient consent, transparency or protection around data use. Vast troves of Nepali citizens' information ranging from names and biometrics to browsing history, purchases and location data are being harvested through digital platforms and systems. This article analyzes the policy gaps around safeguarding citizens' data privacy rights in Nepal. It highlights real-world cases of harms arising from lack of governance around citizens' data, including electoral manipulation, data breaches, unregulated cross-border data transfers and privacy violations during the pandemic under the guise of public health response. For instance, the Cambridge Analytica scandal revealed how private firms can covertly harvest citizens' Facebook data to psychologically profile voters and target them with customized disinformation to influence their behavior. The article argues that forward-looking and rights-based data protection legislation on par with global benchmarks has become an urgent democratic imperative if Nepal is to secure its citizens' privacy, autonomy and choice in the digital age. Comprehensive governance setting clear consent requirements, purpose limitations and penalties around collection and use of citizens' data can no longer be delayed, as Nepal lags behind many of its regional peers in enacting such safeguards. The article makes the case for recognizing data protection as a 21st century freedom struggle to reclaim citizens' rights in virtual spaces in the age of surveillance capitalism.[1] Enacting strong data privacy law is positioned as essential for equitable digital development in Nepal.

Keywords: *Data, Development, Root, System, Privacy.*

I. Introduction

Data is the lifeblood of the digital economy - an intangible yet invaluable asset that fuels and funds businesses, governments and technological innovation today. At its root, data simply

[*] Dr. Newal Chaudhary is a Assistant Professor at Nepal Law Campus, Tribhuvan University, Nepal. The author can be contacted at nc2067@gmail.com.

[1] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Profile Books, 2018.

refers to facts, measurements, statistics, records or observations about the world that have been documented and digitized into a format that computers can store, process and analyze. From the amount of rainfall in a region to census demographics about populations to customer transaction patterns, any quantifiable descriptions about people, events, behaviors or entities in the world become "data" once collected and encoded in binary digits within computational systems. The act of gathering such observational facts from various sources, structuring them into organized databases, deriving insights through statistical modeling and automated analysis, and strategizing further data collection for refinement lies at the heart of what is called "data science" today. Data underpins everything - it is the raw material for artificial intelligence systems to crunch statistical patterns enabling predictive analytics that now customize and personalize various services. Metadata derived from the masses' aggregated data profiles and trails enable companies, governments and researchers to fine-tune their decisions and digital systems in ever more granular fashion seeking convenience, growth or influence at individual and population levels. Thus, an unprecedented quantity and centralization of the world's descriptive information is occurring within networked databases, devices and platforms as processes digitize - everything from finance and commerce to healthcare and entertainment. How this data is collected, stored, connected, accessed, acted upon and governed introduces complex human rights questions in the computer age that existing legal paradigms are only beginning to grapple with as data-driven automation spreads into intimate spheres of human life without historical precedent or consent. Understanding data itself as the oil of the digital economy supplanting industrial assets is crucial context to why its protection merits greater governance. This article employs an interdisciplinary analytical approach drawing on doctrinal legal research around established privacy and consent theories, comparative policy analysis evaluating data protection frameworks globally as benchmarks for Nepal, and empirical case analysis assessing real-world incidents of data exploitation enabled by governance gaps across sectors from elections to education in Nepal. Descriptive data on population-level digital adoption and cyber security risks is sourced from industry reports and media coverage as evidence base to quantify the growing urgency of comprehensive data protection legislation for securing citizens' awareness and control amidst technological transformation. Combining legal principles, policy precedents from neighboring countries, along with recent examples of data harms establishes a robust evidence-driven methodology justifying the imperative for data privacy law to prevent further erosion of Nepal's digital rights landscape. The framework moves from the conceptual foundations around privacy as an inviolable right to operational considerations of notification requirements that could redistribute information asymmetry. This dialectical approach situates data protection as an evolving governance necessity by bridging timeless human rights doctrines with emerging surveillance threats with special resonance in Nepal but global precedents for regulation. A core contention substantiated across cases is how temporary public interest prerogatives around digital response often derogate to permanent privacy erosions once citizen data flows unchecked into centralized repositories lacking robust public accountability. Illustrating this mission creep risks across public health, electoral and education domains makes a rights-based argument for urgent legislation in Nepal before more irreversible data harms take root through global precedent of tech-enabled threats outpacing policy guardrails. The Hacker Hunt Operations, which was performed by the cyber bureau of Nepal in 2020, was able to arrest 19 years old for leaking the database of a popular online food company (FoodMandu). Data, which today has become a sword to kill or to defect anyone in this world. In the digital age, vast amounts of personal data are being collected about individuals by both governments and private companies. This includes information like names, demographics, browsing history, location, communications and more.

While data can provide conveniences like personalized services, there are also risks like privacy violations, profiling, and misuse without proper governance. Major educational technology (EdTech) platforms like Byju's, Unacademy, and Classplus require students to provide personal information during signup including names, contact details, school information, and educational performance data. According to a 2021 report by Mozilla, many EdTech apps capture sensitive student information for profiling and targeted advertising without transparency or consent[2]. Data points can include test scores, attendance records, assignments, and engagement analytics. As Nepal rapidly digitizes, vast troves of citizens' personal data are being generated and harvested by the government and private companies through digital services, social media, e-commerce, and surveillance systems. The government launches a new digital ID system called the National Identity Platform (NIP) which contains biometric data like fingerprints and iris scans as well as demographic data. This sensitive personal data can be used for services like welfare benefits, tax filing, etc. Major e-commerce sites and payment apps like Daraz, Fonepay, and eSewa require users to provide personal information like names, contact details, addresses and financial information. This data can be used for marketing purposes or sold to third parties. Social media platforms like Facebook and TikTok which are widely used in Nepal require real name registration. They collect data on users' posts, friends, interests which can be monetized for advertising. ISPs and mobile providers are mandated to collect SIM registration with ID proof. Call records, locations and texts can be monitored by tapping phones without consent. KYC requirements force citizens to submit personal documents like citizenship, license, etc. to use any digital financial services. Data like ID numbers, photos and biometrics are entered into databases. According to a January 2022 report by DataReportal, over 11.51 million Nepali internet users were on platforms like Facebook, TikTok, and YouTube[3]. These platforms require personal information like names, emails, phone numbers, interests, photos, and more during registration. They then exploit this behavioral data for targeted advertising purposes without sufficiently protecting user privacy or obtaining meaningful consent[4]. For example, Facebook's algorithms can infer details like users' preferences and habits from their likes , shares, and browsing activity in order to serve tailored ads. However, there are concerns about how secure this personal data is, whether users fully understand how it is used, and the lack of control they have.

Private telecommunications companies (Telcos) hold call detail records of millions of subscribers in Nepal. For example, major mobile operators like Ncell and Nepal Telecom have access to usage details for all SIM card owners including call logs, locations, texts messages, and browsing data. This subscriber information is required to be registered at the time of SIM purchase with a government ID per regulation. However, privacy advocates have raised concerns about the security of this data, lack of informed consent, and potential for misuse or unauthorized access without sufficient oversight. Proper procedures and governance need to be ensured to protect citizen privacy while balancing utility of this data for legal purposes like law enforcement investigations. Covid-19 forced increased data collection across healthcare, vaccine registration and contact tracing domains. However, Nepal still lacks a dedicated data protection law establishing clear consent requirements and use limitations around citizens' data. This policy failure leaves

2 Igor Bonifacic, 'Report finds remote learning apps collected and sold kids' data', *Engadget*, 26 May 2022, available at https://www.engadget.com/human-rights-watch-kids-data-183055475.html, accessed on 25 November 2023.

3 Simon Kemp, 'Digital 2022: Nepal', *Datareportal*, 15 February 2022, available at https://datareportal.com/reports/digital-2022-nepal, accessed on 7 November 2023.

4 Ben Smith, 'How TikTok Reads Your Mind', New York Times, 5 December 2021, available at https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html, accessed on 25 November 2023.

Nepalese exposed to potential mass exploitation, commodification and misuse of their personal information by opaque state and corporate interests. Recent incidents reveal the real-world impacts of lacking robust data protection[5]. At its core, enacting data protection legislation recognizes informational privacy as an inviolable human right that promotes citizens' dignity and autonomy against external interests that seek outsized access for data extraction or surveillance. The legal theories underpinning privacy interests limit third party access to personal data in order to secure individual decisional autonomy free from manipulation, coercion or conditioning. Transparency obligations aim to redistribute information power asymmetries between state authorities, corporate interests and citizens by mandating disclosures around data systems that impact people's rights. Disclosure requirements regarding data collection or **algorithmic**[6] processing uphold the consent principles central to liberal democracy so that citizens retain awareness and choice around systems automated to profile, categorize or optimize their interests, behaviors or opportunities often without accessible contestation channels. Ethical data governance further obligates entities gathering citizens' digital exhaust passively and at population scale to ensure voluntariness, fairness, accountability and proportionality checks against unchecked technology deployment. Thus, data protection legislation recognizes dignity, agency and welfare rights with special urgency given the unprecedented scale of behavioral data harvested automatically today through ambient computing infrastructures like mobile devices, platforms and internet-of-things sensors embedded ubiquitously across public and private environments. Its multidisciplinary foundations span long standing privacy theories, emerging platform governance accountability frameworks as well as research ethics considerations around situational power, purpose creep risks and vulnerable population safeguards in the age of surveillance capitalism's relentless data extraction market imperatives.

II. The Pandemic's Impact on Privacy Rights

The COVID-19 pandemic has delivered an unprecedented shock to public health systems and human rights norms globally due to the urgency of responding to an unpredictable crisis. However, many governments capitalized on the state of emergency to rapidly expand their citizen surveillance and data collection programs in ways that weakened privacy safeguards, perhaps permanently even beyond immediate public health necessity. Nepal was no exception to this pandemic-enabled mission creep eroding civil liberties. Under the imperative need for testing, contact tracing and coordinating vaccine delivery to millions in response to the health crisis, various Nepali agencies across health, immigration and statistics bureaus compelled citizens to provide extensive personal data including travel history and medical status without appropriate transparency or consent protocols regarding data protection. Once submitted into centralized databases, citizens had no control or assurances over how this sensitive information spanning health records to biometrics would subsequently be retained long-term, processed by automated systems or shared with third parties absent proper governance. In the absence of rights-based checks or accountability around handling of intimate data provided under duress, there were

[5] Andre Camillo, 'Real life Consequences and examples of Data breaches, some industry Insights and Some tips to reduce risk', *Geek Culture*, 15 October 2022, available at https://medium.com/geekculture/real-life-consequences-and-examples-of-data-breaches-some-industry-insights-and-some-tips-to-3dff9638fdf7, accessed on 25 November 2023.

[6] In the context of cybersecurity, this includes anything from a simple set of rules for identifying spam to a complex machine learning algorithm for detecting advanced cyberattacks.

no guarantees preventing citizens' data from being merged with other datasets, deployed for unauthorized profiling or surveillance agendas beyond public health needs, or sold to private sector data brokers seeking marketing insights without explicit permissions. The excuse of emergency response temporarily normalized disregard for data privacy rights across Nepal much like globally. For instance, agencies like the UK Health Security Agency made patient data accessible to third parties like Amazon and Microsoft cloud-based systems for storage and analytics without appropriately robust controls over future data use rights. Russia's IT giant Yandex collected movement data of Russian citizens across cities to power real-time pandemic dashboards illustrating population flows without transparent limits preventing other exploitation.

Once out of the hands of individuals and centralized into large databases, whether health records or contact tracing apps, citizens lacked assurance of how their personal data would subsequently be extracted, interconnected and utilized by data models to infer behavioral insights, predict risks, cluster populations and enable profiling - well beyond responding to the immediate health crisis. Personal data, once digitized, can be effortlessly reproduced, shared widely, merged across other datasets both private and public to reveal deeper insights about people without their awareness much less consent. Such data retention ambiguity, integration risks across siloes and function creep conflicts directly with principles of purpose limitations and data minimization that rights-based data governance frameworks emphasize. For instance, several governments globally mandated use of contact tracing apps, vaccine certificates and health status passports to track exposure risk and grant access to public spaces - all collecting location, health records and other intimate data with assurances of deletion once the crisis is over. In practice, such temporary emergency surveillance measures targeting a specific crisis like the pandemic laid the groundwork for more permanent erosion of data privacy rights post-health crisis by normalizing mass collection of citizens' sensitive personal information for centralized data mining. The absence of rights-based data protection legislation in Nepal enabled such crisis-fueled precedent of disregard for consent requirements, purpose boundaries or deletion guarantees around citizens' data to become entrenched through data governance gaps, making it harder to reverse after-the-fact. Once datasets are compiled even for legitimate public priorities, removing information already shared with third party processors, interconnected across location data siloes and utilized by predictive analytics prove near impossible to guarantee due to the inherent reproducibility of digital data. Comprehensive legislation with citizens' data rights safeguards before emergence of new threats is the only structural mechanism that could have enforced reasonable limitations, sharing protocols, transparent consent requirements and accountability around agencies handling citizens' sensitive data during the pandemic - both limiting immediate harms and preventing long term mission creep. Its continued absence post-health crisis keeps the door open for abuse of citizens' data harvested under the pretense of public priorities but utilized for unauthorized surveillance, profiling, manipulation or other hidden agendas without oversight accountability. Ceding unchecked power for state authorities to leverage public health emergencies against civil liberties by justifying mass seizure of medical data, location history and biometrics without informed consent requirements or sharing limitations sets a problematic precedent for the future. Excess surveillance infrastructure forged to tackle temporary threats like viruses can too easily be misappropriated for political agendas once entrenched if not decommissioned, as historical examples like post 9-11 PATRIOT ACT overreach demonstrates[7]. Pandemic exigencies must not permanently erode data privacy norms necessary for agency and dignity.

[7] The Patriot Act modernized our ability to monitor criminal and terrorist communications by applying our wiretap laws to new technologies such as cell phones and e-mail without modifying or reducing the legal and constitutional restraints applicable to those tools.

III. Risks from Cross-Border Data Transfers

Nepal's emerging digital economy has seen domestic startups acquired by foreign tech giants, with implications for citizens' data privacy. For example, China's Alibaba bought a majority stake in Nepal's homegrown e-commerce company Daraz in 2017. This transferred control of Nepali users' personal information, like names, contact details and purchase history, to servers located abroad. However, Nepal's regulators lacked clear legal powers to intervene or enforce data localization standards during these cross-border acquisitions[8]. Data profiles, behaviors, conversations, biometrics and more can be exploited, monetized or manipulated for profit, influence or discrimination by opaque algorithms, AI systems and data brokers. For instance, Nepal lacks measures like **Europe's General Data Protection Regulations (GDPR)**[9] that impose steep fines amounting to 4% of global revenue on entities that transfer EU citizens' data outside the EU unlawfully. In the absence of such disincentives, overseas tech giants have been acquiring Nepali startups to gain backdoor access to Nepali users' data through mergers and acquisitions. Once data leaves Nepal's borders without localization protections, citizens lose control over how it gets handled. Rapid technological innovation coupled with increased data-sharing amongst private and public bodies generates various societal benefits but also raises privacy concerns[10]. Data transfer abroad without Nepalese' informed consent compromises their digital rights. While news reports and media analysis reveal emerging real-world data exploitation incidents across Nepal absent commensurate governance, legal and policy scholars have substantiated core data protection deficiencies through systematic research illuminating policy gaps. From assessing citizens' data privacy perceptions regarding institutional handling across healthcare and government agencies to evaluating IT policy readiness through indicators like breach disclosure laws, encrypted data norms and regulatory independence , domain experts argue comprehensive legislation in Nepal continues lacking compared to global rights-based benchmarks. Comparative analyses also position the absence of cohesive data protection frameworks as a key barrier to fostering citizens' trust and digital adoption - whether in contrasting e-government readiness across South Asian countries or examining rider privacy perspectives on transport apps Literature reviews situate Nepal among nations lacking data privacy laws proportional to emerging surveillance threats spanning state, institutional and corporate actors - necessitating stronger consent requirements and enforcement capacities protecting consumers. This policy gap persists despite research by Nepal-based scholars evidencing citizens' data vulnerability across various digital domains and advocating reforms in line with global standards[11].

IV. Cambridge Analytica Scandal Highlights Real-World Harms of Data Misuse

The Cambridge Analytica scandal clearly demonstrated how such cross-border data risks translate

---

8 Newal Chaudhary, 'Data vulnerability in Nepal', *The Kathmandu Post*, 18 October 2023, available at https://kathmandupost.com/columns/2023/10/18/ data-vulnerability-in-nepal, accessed on 25 November 2023.

9 Human Research Protection Office, 'European Union General Data Protection Regulation (GDPR)', *University of Pittsburgh*, available at https://www.hrpo.pitt.edu/european-union-eu-general-data-protection-regulation-gdpr, accessed on 25 November 2023.

10 Brad Greenwood and Paul M. Vaaler, 'Do US State Breach Notification Laws Decrease Firm Data Breaches?' *Minnesota Legal Studies Research Paper*, 2023, available at SSRN: https://ssrn.com/abstract=3885993, accessed on 25 November 2023.

11 Aniket Kesari, 'Do Data Breach Notification Laws Work?', *SSRN*, 2022, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4164674, accessed on 25 November 2023.

into real-world harms when misuse goes unchecked. A UK firm illicitly acquired Facebook data of up to 50 million[12] users globally, including Nepali citizens' data, to psychographic-ally profile voters and target them with customized disinformation to influence their behavior. In the absence of an empowered data regulator, no impartial investigation occurred into alleged unethical influencing of voters through profiling and disinformation in Nepal's 2017 elections[13]. The Election Commission lacked capacity or authority to audit or penalize such data-driven campaign manipulation. Nepali citizens' data was essentially weaponized against their own interests by external actors with impunity[14] due to the policy vacuum on data protection. Democracy is predicated on citizens making free and informed choices at the ballot. Data-driven amplification of disinformation to psychologically manipulate voters directly undermines this agency. Cases globally show how citizens' data can be weaponized at scale when data surveillance and targeting powers are left unregulated. Russia allegedly employed similar tactics in the 2016 US elections[15]. Data protection legislation is urgently required to mandate transparency in political advertising, audits of ad targeting and disinformation campaigns, and penalties for voter manipulation through unethical data harvesting and micro-targeting. Independent electoral oversight of data-driven campaigning practices is essential to secure free and fair digital elections. Otherwise, opaque computational propaganda techniques can hijack and undermine democratic processes.

V. Recurring Data Breaches Reveal Lack of Security Standards

Nepal's recurrent data breaches also highlight gaps in data security. In 2020, private data of over 170,000 Vianet users was leaked[16], including names, phone numbers, addresses, and location data. Similarly, in 2021, over many NTC customers' data were compromised, including financial account details, and call details that enable digital fraud and privacy threat[17]. In the Absence of data security standards, Nepal Telecom faced no robust penalties from any empowered authority for such negligence that irreversibly compromised citizens' data. Customers lacked remedies to hold firms accountable or seek damages. The leaks revealed Vianet and NTC lacked organizational measures to anonymize customer data internally through access controls and encryption. Minor breaches go unreported in the absence of breach disclosure requirements. Data protection legislation would mandate privacy impact assessments for large-scale data processing, anonymization requirements, IT security protocols, access controls, data minimization, encrypted storage, staff training, and regular audits by a supervisory authority. Ireland's Data Protection

12 Carole Cadwalladr & Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' *The Guardian*, 17 March 2018, available at https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, accessed on 25 November 2023.

13 Chaudhary (n 7).

14 Chaudhary (n 7).

15 Abigail Abrams, 'Here's What We Know So Far About Russia's 2016 Meddling', *Times*, 18 April 2019, available at https://time.com/5565991/russia-influence-2016-election/, accessed on 25 November 2023.

16 Kathmandu Post, 'Vianet suffers data breach, leaking personal customer details online', *The Kathmandu Post*, 8 April 2020, available at https://kathmandupost.com/national/2020/04/08/vianet-suffers-data-breach-leaking-personal-customer-details-online, accessed on 25 November 2023.

17 Indo-Asian News Service, 'Nepal Telecom call details stolen by Chinese hackers', *Economic Times*, New Delhi, 13 July 2021, available at https://ciso.economictimes.indiatimes.com/news/nepal-telecom-call-details-stolen-by-chinese-hackers/84366159, accessed on 25 November 2023.

Commission has imposed record euro 525 million penalties on Facebook's WhatsApp and euro 405 million fine on Instagram for GDPR violations. Such deterrence is missing in Nepal.

VI. Scope of Data Exploitation Will Only Grow with Digital Adoption

As digital adoption rises across services from e-governance to e-commerce, fintech to EdTech, the scope and scale of citizen data exploitation will only grow exponentially. More intimate aspects of Nepali citizens' lives, conversations, movements, purchases, interests and networks are coming under round-the-clock algorithmic surveillance without their awareness. Unregulated mass data collection is dangerous. It creates asymmetric power dynamics where state and corporate interests know everything about citizens but citizens know little about how their data is handled. Opaque decisions affecting citizens' rights and lives can be made purely based on their data profiles. Mass data centralization also increases security risks. The state's inherent information and power asymmetry over citizens grows. Politicians and businesses can micro-target users with personalized nudges and emotionally manipulative content optimized to exploit mental vulnerabilities. Opaque algorithmic decisions can entrench biases, widen inequalities and undermine human dignity. Unethical experiments like Facebook's mood manipulation[18] study show how tech firms can deliberately influence users' emotions at scale without consent when data exploitation goes unchecked. The threat of mass persuasion and control through data merits robust protection.

VII. Comprehensive Legislation Needed to Secure Data Rights

Clearly, comprehensive legislation is urgently required to mandate informed consent requirements, mandatory anonymization, purpose limitations, and tough penalties like large fines for violations. Citizens' data must be collected minimally, used for limited purposes disclosed explicitly, retained briefly, and shared only after explicit consent. Vulnerable groups like children merit higher protection. An independent statutory data regulator must also be set up to enforce citizens' data rights and regularly audit data handling practices. Funding for the regulator could come from a portion of mandatory data protection fees levied on large data processors like banks, Telco's and tech companies annually, as practiced in the EU[19] . Such a rights-based approach to data governance is increasingly a global norm. Unlike many of its regional peers, Nepal currently lacks a comprehensive data protection law. While Nepal has made piecemeal gestures towards data privacy across laws like the Electronic Transactions Act 2006, National ID and Civil Registration Act 2019, and various data provisions from the Nepal Rastra Bank for financial sectors, experts argue these remain fragmented and limited in scope compared to the scale of emerging privacy threats warranting an overarching data protection law. For instance, the e-commerce bill tabled in Parliament focuses narrowly on regulating online businesses and lacks comprehensive safeguards

[18] Robinson Meyer, 'Everything We Know About Facebook's Secret Mood-Manipulation Experiment', *The Atlantic*, 28 June 2014, available at https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/, accessed on 25 November 2023.

[19] Ryan Browne, 'Europe and the U.S. finally agree a landmark data-sharing pact — and it's already under threat', *CNBC,* 12 July 2023, available at https://www.cnbc.com/2023/07/12/eu-and-us-agree-new-data-sharing-deal-what-is-it-and-why-it-matters.html, accessed on 25 Nov 2023.

empowering consumers against risks like unauthorized data collection or sales to third parties once shared for digital transactions. Proposed bills around digital payments and settlement laws enacted by Nepal Rastra Bank similarly emphasize orderly processing of financial transactions without corresponding assurances around citizens' awareness, control over data trails generated or accessible redressal against corporate data misuse once submitted even for defined purposes. While sector-specific regulators attempt risk bounds around industry data use, baseline universal privacy protections strengthened through proactive rights-based checks remain absent - including mandatory disclosures around data harvesting, algorithmic transparency requirements with plain language explanation of automated decisions impacting consumers, opt-out protocols without punitive reprisals or steep penalties amounting to significant percentage of annual turnover against negligent actors or malicious violations across private and public sectors.

VIII. Core principles of data protection law

1. **Purpose Limitation**: This principle restricts data collection and use to specific, legitimate purposes explicitly communicated to the data subject (the person whose data is being handled). Organizations cannot collect or use data for anything beyond those stated purposes without further consent.

2. **Imagine**: You provide your email for a newsletter subscription. Purpose limitation means they can't use it for marketing unrelated products without your okay.

3. **Data Minimization:** This principle emphasizes collecting and using only the minimum amount of data necessary for the intended purpose. Organizations should avoid gathering excess or unnecessary personal information.

4. **Think:** A fitness app tracking your steps doesn't need your political affiliation. Data minimization protects against irrelevant data collection.

5. **Storage Limitation:** This principle dictates that personal data should not be kept for longer than necessary to achieve the intended purpose for which it was collected. Organizations must have procedures for safely deleting or archiving data no longer required.

6. **Picture:** Medical records might need longer storage compared to online shopping preferences. Storage limitation ensures data is not held indefinitely without justification.

These are just three of the many important principles in data protection law, but they offer a solid foundation for understanding how personal information should be handled responsibly and ethically. This reactive regulatory approach fails to respond adequately to documented cases of unauthorized exploitation of Nepali users' data for opaque profit or influence - whether EdTech apps profiling students for targeted advertising based on their learning performance data scraped without consent, social media platforms covertly allowing electoral manipulation through psychographic propaganda crafted using personal data trails, law enforcement agencies normalizing access to citizens' digital exhaust like real-time location history and biometrics through mobile carriers without judicial limitations, or recurring negligence enabling data breaches across telecom and internet service providers absent major disincentives. Hence, merely expanding the scope of existing laws without overhauling their rights-based foundations limits

their efficacy to govern new frontiers around citizens' data privacy and algorithmic accountability issues that now arise daily. As more intimate decisions, services and opportunities migrate online, comprehensive forward-looking data protection legislation future-proofed to evolve alongside technological transformations becomes urgent and overdue. Neighboring countries like India, Thailand, Taiwan, Sri Lanka, and Pakistan have already enacted forward-thinking policies and regulations to safeguard citizens' personal data. For example, India passed the Digital Personal Data Protection (DPDP) Act 2023 .Sri Lanka established its Data Protection Act in 2021 after a multi-year process. In contrast, Nepal is still in legislative drafting stages without an operational framework in place. This policy gap places Nepal behind its neighbors and international data protection standards. Enacting a progressive law tuned to the digital age remains a pressing priority for the country. India's data privacy law draws inspiration from the EU's GDPR, which is regarded as the gold standard for its strong citizen rights safeguards. Even the US is actively considering a national data privacy act. But the Nepali government has shown a lack of urgency to legislate data protection despite repeated controversy and harm. The Supreme Court is yet to even definitively affirm privacy as a fundamental constitutional right, leaving ambiguity around basic digital rights[20]. This delay enables unchecked harm as citizens' lives, choices and liberties migrate online without commensurate legal safeguards. All stakeholders must make data protection an urgent legislative priority.

IX. Data Protection as a Democratic Imperative

Nothing less than citizens' rights, dignity and empowerment in the digital age is at stake. Data is power[21]. Unregulated mass data collection creates information asymmetry that inherently disempowers citizens. Opaque state surveillance strips citizens of their right to privacy, freedom of thought and personal liberty. It threatens democracy itself. Data protection aims to redistribute information power and prevent unchecked mass surveillance capitalism. It asserts citizens' rights to control their data, demands transparency in data systems impacting them, and holds entities accountable for data misuse. Thus, the data protection crusade has deeper democratic foundations beyond just privacy - it upholds citizen participation, informed choice, accountability, and threats to these pose far greater long-term costs than any temporary growth dividends from unchecked data extraction. Data protection is essential for equitable digital development. Nepal cannot afford further erosion of digital rights through inaction. It must fulfill its responsibility to robustly safeguard citizens' privacy, dignity, and autonomy in virtual spaces through progressive legislation on par with global standards. Enacting data protection now will also boost Nepal's IT sector competitiveness. India's privacy law is driving IT investments as global clients prefer jurisdictions with data protection assurances[22]. Data localization regulations that mandate sensitive citizen data remain stored on servers physically located only within Nepal's geographical borders also carry significant economic benefits that directly contribute to domestic job creation. By requiring digital companies across finance, healthcare and other critical sectors that gather large citizen data banks on customers to invest in in-country data

[20] Chaudhary, (n 7).

[21] Chaudhary, (n 7).

[22] Ali A. Jessani & Kirk J. Nahra, 'India Passes Long-Awaited Privacy Law', *WilmerHale*, 18 August 2023, available at https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20230818-india-passes-long-awaited-privacy-law, accessed on 25 Nov 2023.

storage infrastructure, substantial expansion of Nepal's technology industry gets incentivized through fulfillment roles. Cloud engineers, database administrators, cyber security analysts, data governance personnel and other IT jobs in high demand today get boosted rather than letting such positions trickle abroad by allowing uncontrolled data transfers to overseas servers on foreign soil without commensurate returns for Nepali youth. India's experience bears this out. After the Indian government began tightening localization requirements forcing global players providing payment services, e-commerce platforms and health apps to keep Indian customer data storage restricted within the country since 2019 rather than solely self-regulated foreign servers, subsequent data center investments expanded rapidly. Google opened its second India cloud region to meet regulatory obligations while Amazon Web Services similarly announced plans for installing data centers across multiple Indian metro regions for client data processing in compliance with emerging cross-border data transfer restrictions. This created local data infrastructure jobs from hyper scale storage construction to cloud management roles for hordes of digital economy workers rather than concentrating data-driven tech industry opportunities solely in distant American metros. The Indian IT industry's trade groups like NASSCOM[23] estimated data domiciling priorities boosted demand for specialized data security and storage talents overseeing proper controls around citizen data by over 50% illustrating localization's employment dividends. Without binding governance requiring foreign tech firm's route data traffic through in-country servers, such jobs stood at higher flight risk to concentrate abroad instead. Balanced data localization quotas alongside comprehensive governance establishing citizens' data rights serve crucial interlocking purposes for democracies navigating complex digital transitions – preserving both prosperity and civil liberties instead of dichotomizing the two. Beyond economic gains, responsible data sovereignty powers participation in automation on people's terms rather than leaving societies digitally colonized through asymmetric information flows. Cross-border data transfers cannot remain the path of least corporate resistance without corresponding data security, infrastructure investments and job opportunities returning equitably back to Nepal once foreign tech giants gain unconstrained access to Nepali citizens' offline and online digital footprints. Data protection balanced through reasonable localization is no longer a distant aspiration but an immediate democratic imperative if Nepal is to sustainably progress all dimensions of equitable development in the 21st century. Enacting data protection recognizes privacy as an inviolable human right that promotes citizens' dignity, autonomy and choice against external interests that seek disproportionate access for data extraction or surveillance. Without checks against states, companies and institutions that encode growing aspects of socio-economic participation digitally across services from welfare benefits to credit scoring, vast information and power asymmetry gets created allowing external parties disproportionate visibility into people's lives without commensurate transparency obligations. Core rights impact span freedom of thought, expression, dissent and assembly if people perceive persistent monitoring of their browsing or communication content that could gauge behavioral insights or predictively profile based on their digital exhaust passively recorded simply from participating in digitized social systems. Data protection aims to bound such ambient surveillance and lay accountability guarantees by mandating purpose limitation around data uses disclosed explicitly at collection

[23] NASSCOM stands for the National Association of Software and Service Companies. It is a nonprofit trade association and advocacy group focused on the information technology and business process outsourcing industry in India. NASSCOM is the premier trade body and industry association for India's technology and digital services sector acting as a key platform for market growth, policy advocacy, partnerships and skills building across the country's burgeoning IT-BPM industry. It plays a strategic role in steering the rapid development of India's globally competitive technology services industry.

time, enforcing revocation protocols without reprisals if consent gets withdrawn later and instituting external audits to assess rights impacts of automated decisions made around citizens' opportunities or access to services based on their data traces. More broadly, data sovereignty establishes participatory parity for citizens over technology deployment through collective oversight over cross-border data flows. It prevents exploitative scenarios where foreign corporate interests influence domestic groups for outsized data extraction gains using persuasive and personalized propaganda crafted from illegally obtained private profiles. Thus, data protection and localized governance facilitates equitable digital development built on human rights.

X. Analysis and Conclusion

The rapid digitization of services across Nepal makes enacting strong data protection legislation an urgent democratic priority. Comprehensive governance setting consent requirements, purpose limitations and deterrence mechanisms around citizens' data can no longer be delayed if the nation is to secure Nepalese's rights in virtual spaces, uphold their dignity, and prevent mass disempowerment through unfettered surveillance. With increasing ubiquity of digital platforms across finance, education, healthcare and commerce, vast troves of citizens' personal information now flow into opaque government databases and corporate data warehouses on a 24x7 basis often without their meaningful consent or awareness. Intimate aspects of Nepali citizens' lives – their conversations, movements, transactions, browsing habits, photos and emotional states – are coming under round-the-clock monitoring powered by intrusive data collection and analytical systems. Once pooled, this digitized data can be effortlessly reused, retained indefinitely, merged across datasets and mined in unexpected ways that citizens cannot foresee or consent to. Such exponential information asymmetry skews power dynamics against citizens' agency and awareness regarding automated decisions and persuasive systems shaping their choices and lives behind the scenes. Opaque state or corporate interests can deploy citizens' data to micro-target them with emotionally manipulative content, entrench biases through algorithms, make consequential decisions about their rights, welfare or opportunities based on their digital profiles without accountability, or covertly influence their behavior at scale as the Cambridge Analytica scandal revealed. Unchecked, such impersonal data-driven "surveillance capitalism" holds deeply dehumanizing and anti-democratic possibilities in its quest to predict and produce desired consumer outcomes. It threatens citizens' awareness, autonomy and dignity. Even apparent conveniences like personalized services can normalize erosion of decisional privacy and encourage self-censorship that undermines dissent. Data protection aims to redistribute information power and make such automated systems impacting rights transparent and contestable, not eliminate technological progress itself.

The unprecedented scale and scope of data extraction enabled by digitization makes comprehensive governance protecting Nepali citizens' privacy while balancing legitimate interests cannot be delayed any further. The policy costs of inaction are rising daily. For one, citizens are left dangerously exposed to identity theft, fraud, profiling, manipulation or loss of opportunities due to recurring data breaches resulting from the lack of security standards, access controls or punitive deterrence. Firms face no strong disincentives against negligence, preventing accountability. Once private data leaks out, it cannot be contained back. Similarly, citizens lose control over their information once it transfers abroad after foreign takeovers of Nepali startups. Unlike jurisdictions like the EU with strong cross-border data transfer protections and localization

requirements, overseas tech giants have been acquiring Nepali digital firms to access local user data with impunity. Micro-targeting for profit or influence can subsequently occur without oversight. The pandemic also revealed how citizens' sensitive health data around tests, contacts and vaccines was collected en masse without transparency by various agencies. Once centralized in databases, such intimate information can be reused or merged to enable surveillance well after the public health crisis recedes. Thus, temporary emergency measures can have lasting rights impacts without checks against mission creep. Legislating data protection is no longer just a distant aspiration but an urgent obligation to secure Nepali citizens' awareness, agency and welfare in rapidly evolving algorithmic systems mediating their lives. The profound power and information asymmetry such technologies introduce require balanced governance and democratic oversight to prevent abuse. Checks and balances are always essential where technological transformations concentrate power or outpace ethical evolution. Comprehensive data protection law in line with global rights-based benchmarks can place reasonable constraints upon unfettered data extraction and commodification by mandating informed consent requirements, storage limitations, purpose boundaries, strong anonymization norms, opt-out rights, algorithmic transparency requirements, mandatory security protocols, empowered regulatory auditing capacities, steep penalties for violations and accessible redressal mechanisms. Such forward-looking digital rights safeguards uphold citizen participation, trust and accountable innovation in emerging technologies rather than arbitrarily restricting progress. Data protection aims to democratize the digital economy, not banish it through Luddite prohibitions. It redistributes information privileges to prevent asymmetry. Nepal has the opportunity to lead through progressive legislation. Fashioning consensus between state, business and civil society is key to a balanced law attuned to the data-driven century. Indeed, data protection deserves urgent multi-partisan support as a 21st century freedom movement to reclaim citizens' awareness, consent and control against disempowering systems. Its democratic foundations aim to redistribute information power between state, market and citizens. Much like labor rights movements arose against 19th century industrialization harms, data rights struggles are essential for equitable development of 21st century digital economies by empowering citizens' participation within technologies profoundly impacting their lives and freedoms. Data protection merits recognition as the new frontline to uphold civil liberties, welfare, agency and human rights against technological threats. Its time has come in Nepal. The future trajectory of citizens' privacy, autonomy and digital rights hangs in the balance. Comprehensive legislation carries far greater long-term benefits for digital development than any temporary dividends from unfettered data extraction devoid of rights-based checks. 21st century progress itself requires balanced evolution of governance, ethics and technology in step rather than blind accelerations. The Nepal government must recognize this principle and make data protection a legislative priority for the Digital Nepal vision to equitably uphold all citizens' participation and awareness within rapidly evolving technological spaces mediating their lives and rights. In conclusion, as we embrace the transformative power of digital progress, it is imperative to ensure that technology evolves hand in hand with rights-based governance and democratic values, safeguarding against the risks of overreach and preserving the foundations of a just and inclusive society.