मिडिया मोनिटरिङ्ग

अनुगमन प्रतिवेदन २०८१

नेपालमा डिजिटल अधिकारको अवस्था: एक समिक्षा

Body & Data

लेखन: विवेक वर्णवाल
सम्पादन: अनिषा (अनिकर्म), नुभा राई, दोभान राई
लेआउट: श्रीजीत राजभण्डारी
कभर: मोनीषा चौधरी

प्रकाशन: बडी एण्ड डाटा
सहयोग: भिजन फर चेन्ज

सम्पूर्ण आधिकार बडी एण्ड डाटा संग सुरक्षित
बडी एण्ड डाटा , २०२५

Body & Data

२०१७ मा स्थापित बडी एण्ड डाटाले सबैका लागि पहुँचयोग्य, सुरक्षित र न्यायपूर्ण डिजिटल क्षेत्रको परिकल्पना गर्दछ। बडी एण्ड डाटा नेपालको सन्दर्भमा डिजिटल अधिकारहरूमा केन्द्रित भएर अन्तर–आन्दोलन निर्माण, सूचनामा पहुँचका लागि सहजीकरण, तथा ज्ञान निर्माणको काम गर्छ।

बडी एण्ड डाटाको मुख्य लक्ष्य महिला, क्वियर व्यक्तिहरू र सीमान्तकृत समुदायबीच डिजिटल अधिकारसम्बन्धी बुझाइ र सूचनाको पहुँच विस्तार गर्नु हो, जसले गर्दा उनीहरूले सुरक्षित र न्यायपूर्ण डिजिटल वातावरणमा आफ्ना अधिकारहरू पूर्णरूपमा प्रयोग गर्न सक्छन्।

Established in 2017, Body & Data works to enhance understanding and access to information on digital rights among women, queer people and marginalized groups where they are able to exercise their rights in a safe and just digital space. We work towards the vision of accessible, safe and just digital spaces for all, through cross movement building, facilitation for access to information, knowledge building and dissemination on digital rights in the context of Nepal.

Facebook Instagram Bluesky X

https://www.facebook.com/bodyanddata
https://www.instagram.com/bodyanddata
https://bsky.app/profile/bodyanddata.bsky.social
https://x.com/bodyanddata

www.bodyanddata.org

विषय सूची

१. **नेपाली मिडियामा डिजिटल अधिकारको समिक्षात्मक अवस्था** ---- १

२. **उद्देश्यहरू** ---- ३

३. **अध्ययन विधी** ---- ४

४. **विषयगत अवलोकनहरू** ---- ६

४.१. नेपाली डिजिटल स्पेसमा हाम्रो डाटा गोपनियता र सुरक्षाको अवस्था ---- ६

४.१.१.निजी पहिचान चोरी, आर्थिक ठगी तथा आपराधिक गिरोह ---- ६

४.१.२. बढ्दो साइबर ठगीमा युवाको उल्लेख्य सहभागिता: नेपाल राष्ट्र बैंकको प्रतिवेदन ---- ७

४.१.३. डिजिटल बैंकिंग सेवाभित्र सुरक्षा चिन्ता ---- ७

४.१.४. सरकारी डिजिटल स्ेसमा गोपडनयताको सवाल ---- ८

४.१.५. अन्तर्राष्ट्रिय डिजिटल स्पेसको अवस्था ---- ९

४.१.६. नेपालमा डीपफेक ---- १०

४.१.७. नक्कली प्रहरी इमेल ठगी ---- १०

४.२. 'डिजिटल नेपालका असुरक्षित प्रयासहरु ---- ११

४.२.१ क्रसबोर्डर डिजिटल भुक्तानी सेवा ---- ११

४.२.२. राष्ट्रिय परिचयपत्रको उपयोग विस्तार: डिजिटल समावेशिता कि बहिष्करण? ---- १२

४.२.३. प्रविधिमा अपाङ्गता भएका व्यक्ति बहिष्करणमा ---- १३

४.२.४. नक्कली चालक अनुमतिपत्र प्रकरण: डिजिटल अधिकार र गोपनीयताको चुनौती ---- १३

४.३. प्रविधिमा आधारित हिंसा (अनलाईन भायलेन्स) ---- १४

४.३.१. महिलाविरुद्ध रिभेन्ज पोर्न ---- १५

४.३.२. मधेसी समुदायविरुद्ध नश्लीय द्वेष ---- १५

४.३.३. LGBTQIA+ समुदायविरुद्ध सामाजिक सञ्जालमा नकारात्मक प्रतिक्रिया ---- १६

४. ४. वाक स्वतन्त्रता ---- १७

४.४.१. सीधाकुराको स्टिङ अपरेसन र अदालतको कारबाही ---- १७

४.४.२. टिकटक माथिको प्रतिबन्ध हटाइनु: डिजिटल स्वतन्त्रता कि नियन्त्रण? ---- १८

४ ४.३. गिग अर्थतन्त्र: कन्टेन्ट क्रिएसन ---- १९

५. **ट्रेन्ड, सिफारिसहरू, र निष्कर्ष** ---- २०

१ नेपाली मिडियामा डिजिटल अधिकारको समिक्षात्मक अवस्था

नेपाली मिडियामा वर्षभरि डिजिटल अधिकार सम्बन्धि कस्ता विषयवस्तु, सन्देश र प्रवृत्ति प्राथमिकतामा परे अनि प्रविधि र इन्टरनेटसँग सम्बन्धित हाम्रो मानवाधिकारको स्वरूप कस्तो देखिन्छ भन्ने विश्लेषण र बहस पस्किनका लागि हामीले सन् २०२१ देखि यस समिक्षात्मक प्रतिवेदनको थालनी गरेका हौँ।

मिडिया अनुगमन डिजिटल अधिकारहरू र डिजिटल स्पेसमा लैंगिक, यौनिक तथा सामुदायिक रुपमा समाजमा सीमान्तकृत भएका व्यक्तिहरुको सवालमा समावेशिताका अवस्था बुझ्नका निम्ति महत्त्वपूर्ण छ।

सन् २०२४ को वर्षमा हामीले सरकार र निजी क्षेत्रबाट डिजिटल प्रविधि तथा सेवामा थुप्रै पहलहरू देख्यौं। यद्यपि, यस्ता पहलकदमीहरूमा **समावेशिता, पारदर्शिता र उत्तरदायित्वको कमी** देखिन्छ। साथै **गोपनीयता उल्लंघन, डाटा चोरी, प्रविधिमा आधारित हिंसा र साइबर अपराध**का घटनाहरू पनि बढ्दै गएका देखिन्छन् ।

जस्तै, सरकारले २०२४ मा राष्ट्रिय परिचयपत्रको उपयोगिता विस्तार गर्यो। यस कदमले राज्यद्वारा प्रदान गरिने सेवाहरु डिजिटल गर्दै त्यसमा पहुँच बिस्तार गर्ने उद्देश्य राखे तापनि, यौनिक र लैंगिक विविधताको आधारमा **समावेशिता, गोपनीयता, र सीमान्तीकरणमा परेका समुदायहरूको डिजिटल अधिकार सुनिश्चित भएको छैन।**

त्यस्तै, यस वर्ष महिलाविरुद्ध **रिभेन्ज पोर्नका** घटना बढेको देखिन्छ भने सामाजिक सञ्जालमा मधेसी समुदायले **नश्लीय द्वेष** र लैंगिक तथा यौनिक रुपमा विविध (LGBTQIA+) समुदायले नकारात्मक प्रतिक्रियाका कारण **व्यापक भेदभाव र मानसिक दबाब** झेल्नुपर्यो।

मिडियामा यस वर्ष टिकटकमाथि लागेको प्रतिबन्ध हटेको र टिकटकले पालना गर्नुपर्ने सरकारी नियमनहरु बहसमा रहे।

यस वर्ष सरकारद्वारा टिकटकमाथि लगाइएको प्रतिबन्ध हटाइएको छ र त्यसपछि टिकटकलाई नियमन गर्ने सम्बन्धमा विभिन्न नीति बहसहरू मिडियामा देखिए। तर, यस्ता बहसमा **सामाजिक संरचनाको विश्लेषण, अभिव्यक्ति स्वतन्त्रता तथा डिजिटल स्पेसको प्रयोग अधिकार**को रुपमा कसरी सुनिश्चित गर्न सकिन्छ भन्ने गहन बहसको अभाव देखिन्छ।

मिडियामा प्राय: सरकारको वेबसाइट तथा प्रणालीमा हुने **साइबर आक्रमण**बारे उद्दृत गर्दै **वैयक्तिक गोपनियता र डाटा सुरक्षा**को संदर्भमा सरकारको नीति, काम गर्ने तरिका र कार्यक्षमतामाथि प्रश्न गरेको र व्यापक चासो देखाइएको पाइन्छ। तर, महिला, दलित, आदिवासी जनजाति, यौनिक तथा लैंगिक अल्पसंख्यकहरू जस्ता समुदायका दृष्टिकोणबाट गरिएको विश्लेषण भने न्यून पाइन्छ।

त्यस्तै, महिलाविरुद्ध प्रविधिमा आधारित हिंसा सम्बन्धि reporting एउटा निश्चित 'हार्ड न्यूज' सामाचार संरचनामा सम्प्रेषण हुन्छ भने विचारात्मक तथा खोजमूलक रिपोर्टहरू (investigative reporting) को अभाव देखिन्छ, जसले समस्या गहिराइमा गएर देखाउने क्षमता राख्दछ। टिकटक नियमनको विषयमा पनि सामाजिक विश्लेषण भएको पाइदैन।

यस प्रतिवेदनमा हामीले अनुसूची १ मा उल्लिखित मिडियाहरूको अनुगमनबाट प्राप्त समाचारहरूलाई अनुसूची २ मा उल्लिखित विश्लेषण विधिहरू प्रयोग गरी मूल्याङ्कन गरेका छौँ।

२ उद्देश्यहरू

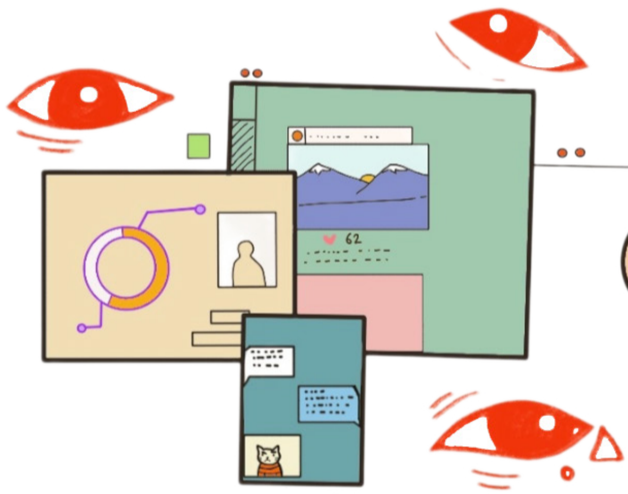
मिडिया अनुगमनको उद्देश्य नेपालमा डिजिटल अधिकारसम्बन्धी अन्तर्दृष्टि प्राप्त गर्न समाचार, बहस र प्रवृत्तिहरूको विश्लेषण गर्नु हो। नारीवादी दृष्टिकोणबाट सञ्चार अनुगमन हेर्दा, यो समाचार, विमर्श र उदीयमान प्रवृत्तिहरूको आलोचनात्मक अध्ययन गर्ने एक शक्तिशाली उपकरणका रूपमा कार्य गर्दछ।

यस किसिमको विश्लेषणले सञ्चार माध्यमहरूले निर्माण गरेका कथाहरू तथा तिनले विभिन्न समुदायहरूमा पार्न सक्ने प्रभावलाई बुझ्न मद्दत गर्दछ। विशेषतः डिजिटल अधिकारका मुद्दाहरूले महिला, क्वियर व्यक्ति, दलित, जनजाति, अपांगता भएका व्यक्ति, तथा अन्य सीमान्तकृत समुदायहरूमा पर्ने असमान प्रभावहरूको पहिचानका लागि यस्तो दृष्टिकोण आवश्यक हुन्छ।

डिजिटल अधिकारको परिदृश्यको आलोचनात्मक विश्लेषणले **सूचित संवाद प्रवर्द्धन गर्न, नीतिगत वकालतलाई बलियो बनाउन, र सतही रिपोर्टिङभन्दा पर जान** प्रेरित गर्दछ। यसले सञ्चार माध्यमहरूमा व्याप्त शक्ति संरचनाहरू, पूर्वाग्रहहरू र असमान प्रतिनिधित्वहरूलाई उजागर गर्न सहयोग पुर्याउँछ।

सञ्चार माध्यममा को बोल्छ, कसरी बोल्छ, र कसका आवाजहरू ओझेलमा पर्छन् भन्ने प्रश्न उठाउन यो अनुगमनले सघाउँछ। यस अनुगमन रिपोर्टबाट प्राप्त निष्कर्षहरू भविष्यमा **सञ्चार संवेदीकरण, डिजिटल अधिकारको प्रवर्द्धन, र बहु-वैकल्पिक आवाजहरूको समावेशी प्रतिनिधित्व**का लागि सशक्त साधन बन्ने अपेक्षा गरिएको छ।

३ अध्ययन विधी



यस प्रतिवेदन मार्फत् सन् २०२४ को वर्षभरी नेपाली सन्दर्भमा डिजिटल अधिकारको समग्र अवस्था कस्तो रह्यो भनी विश्लेषण प्रस्तुत गरिएको छ। यसका लागि मुख्य अनलाइन मिडियामा प्रकाशित डिजिटल माध्यम, इन्टरनेट, प्रविधि, डिजिटल अधिकार, तथा डिजिटल क्षेत्रमा हुने हिंसा जस्ता विषयसँग सम्बन्धित समाचार तथा विचार/विमर्शहरूको अनुगमन, संकलन, अध्ययन र विश्लेषण गरियो। जम्मा ५७४ वटा समाचार र सामग्री संकलन गरिएका छन्, जसमा विगतमा त्रैमासिक रूपमा संक्षिप्त प्रतिवेदनहरू पनि प्रकाशन र संप्रेषण गरिएका थिए।

यस वार्षिक मिडिया अनुगमन प्रतिवेदनमा तीनै त्रैमासिक तथा समग्र अनुगमनबाट आएका मुख्य विषयवस्तुहरूलाई विषयगत शीर्षकमा विभाजित गरी प्रस्तुत गरिएको छ। यस अध्ययनको उद्देश्य नेपाली मिडियामा डिजिटल अधिकारको अवस्थाको आलोचनात्मक पुनरावलोकन गर्नु, प्रवृत्तिहरू पत्ता लगाउनु, र समावेशिताको अभावलाई उजागर गर्नु हो।

Body & Data ले सन् २०२१ देखि मिडिया मनिटरिङ सुरु गरेको हो । हामिले डिजिटल अधिकारसम्बन्धी समाचार, विचार, तथा बहसलाई नियमित रूपमा संकलन, विश्लेषण, र दस्तावेजीकरण गरी मासिक, त्रैमासिक, तथा वार्षिक प्रतिवेदन प्रकाशन गर्दै आएका छौं। मिडिया मनिटरिङको अध्ययन विधि अन्तर्गत, हामी प्रत्येक महिनाको अन्त्यतिर **"मिडिया मनिटरिङ सेयरिङ**

सेसन (MM sharing session)” आयोजना गर्छौं, जसमा सो महिनाभर नेपाली मिडियामा डिजिटल अधिकारसँग सम्बन्धित रिपोर्टिङको अवस्थाबारे समिक्षा र छलफल गरिन्छ। यी छलफलहरूमा डिजिटल हिंसा, सामाजिक सञ्जालमा बढ्दो निगरानी, गोपनीयता उल्लंघन, प्रविधिमा पहुँचको असमानता, तथा कानुनी र नीतिगत विकासहरूका विषयमा आलोचनात्मक नारीवादी दृष्टिकोण र अन्तर्विच्छेदन दृष्टिकोण (intersectional lens) बाट गहिरो विश्लेषण गरिन्छ। यसले जात, वर्ग, लिङ्ग, यौनिकता, पहुँच, तथा भौगोलिक अवस्थाजस्ता परिप्रेक्ष्यहरूको अन्तरसम्बन्धलाई उजागर गर्न मद्दत पुर्‍याउँछ।

यस्ता छलफलहरूबाट उठेका मुख्य विषयवस्तुहरूलाई “मासिक मिडिया मनिटरिङ प्रतिवेदन” मार्फत संकलन गरिन्छ, जुन वार्षिक प्रतिवेदन तयार गर्दा महत्वपूर्ण आधारका रूपमा प्रयोग गरिन्छ। वार्षिक प्रतिवेदनमा ती मासिक तथा त्रैमासिक अनुगमनहरूबाट संकलित सूचनाहरूलाई विषयगत रूपमा वर्गीकृत गरी विश्लेषणात्मक रूपमा समेटिन्छ।

यस वार्षिक प्रतिवेदनको उद्देश्य नेपाली मिडियामा डिजिटल अधिकारको अवस्थाको आलोचनात्मक पुनरावलोकन गर्नु, त्यसमा देखिएका प्रवृत्तिहरू पहिचान गर्नु, र समावेशिताको अभावलाई उजागर गर्नु हो। यस वर्षदेखि, हाम्रा सम्पूर्ण मिडिया मनिटरिङ प्रतिवेदनहरू https://bodyanddata.org/mm/ मा सार्वजनिक रूपमा उपलब्ध छन्। ती प्रतिवेदनहरूले नेपाली मिडियामा डिजिटल अधिकारसम्बन्धी विमर्शहरूको विकासक्रम, प्रवृत्ति, र चुनौतिहरू बुझ्न चाहने अनुसन्धानकर्ता, नीति निर्माता, पत्रकार, तथा अन्य सरोकारवालाहरूका लागि उपयोगी स्रोतका रूपमा कार्य गर्छन्।

नोट : यस अनुगमन प्रतिवेदन Body & Data को संस्थागत पहल अन्तर्गत तयार पारिएको हो। यद्यपि, भुलचुकको सम्भावना रहन सक्छ भन्ने स्वीकार गर्दै, यदि तपाईंहरूसँग कुनै सुझाव वा प्रतिक्रिया छन् भने, कृपया communication@bodyanddata.org मा इमेल गरेर सम्पर्क गर्न आग्रह गर्दछौं ।

४ विषयगत अवलोकनहरू

४.१.

नेपाली डिजिटल स्पेसमा हाम्रो डाटा गोपनियता र सुरक्षाको अवस्था

४.१.१. निजी पहिचान चोरी, आर्थिक ठगी तथा आपराधिक गिरोह

नेपालमा विभिन्न साइबर अपराध र डाटा दुरुपयोगका घटनाहरूले डिजिटल अधिकारको हननलाई थप गम्भीर बनाउँदै लगेका छन्। यी घटनाहरूमा प्रयोगकर्ताको निजी जानकारीको चोरी र संवेदनशील डाटा आपराधिक गिरोहलाई बिक्री गर्ने गतिविधिहरू विशेष रूपमा देखा परेका छन्।

यसै संदर्भमा एउटा प्रतिनिधि घटनाको रुपमा नोभेम्बरमा खल्ती डिजिटल वालेटका तीन कर्मचारी पक्राउ परेका थिए। २० देखि २२ वर्ष उमेरसमूहका उनीहरू ग्राहक पहिचान (KYC) भेरिफिकेसनको जिम्मेवारीमा कार्यरत थिए। उनीहरुले सेवाग्राहीहरूको व्यक्तिगत जानकारी (जस्तै नागरिकताको प्रतिलिपि र तस्वीर) आपराधिक गिरोहलाई उपलब्ध गराएका थिए। यसका कारण ५० भन्दा बढी नक्कली वालेट खाता खोलिएको थियो, जसलाई ठगी र अवैध कारोबारका लागि प्रयोग गरिएको थियो। यस घटनाले प्रयोगकर्ताहरूको निजी जानकारी गम्भीर जोखिममा परेको र कर्मचारी तहमै डाटा सुरक्षामा पर्याप्त निगरानी तथा प्रशिक्षणको अभाव रहेको देखिएको छ।

यस्तै, ठगहरू प्रयोगकर्तालाई खाता नवीकरण र अपडेट गर्ने भन्दै विवरण माग्ने; प्रयोगकर्ताले विश्वास गरी अकाउन्ट नम्बर, जन्ममिति, पासवर्ड र ओटीपी उपलब्ध गराउने र यस्ता संवेदनशील विवरण पाएपछि ठगले उक्त अकाउन्टबाट रकम अन्य अकाउन्टमा ट्रान्सफर गर्ने गरेको पाइएको छ। ठगहरूले नक्कली नागरिकता र चोरी गरिएका कागजातहरू प्रयोग गरी टेलिकम कम्पनीबाट सिम निकाल्ने र सोही सिम प्रयोग गरेर बैंकमा खाता खोल्ने गरेको प्रहरी अनुसन्धानले देखाउँछ।

सिमकार्डको प्रमाणिकरण प्रणालीमा कमजोरी रहेको प्रष्ट हुन्छ। थप, प्रमाणिकरण प्रक्रियामा कमजोरीका कारण सिम डुप्लिकेसन, अरूकै नाममा सिम सक्रिय गर्ने, र पीडित प्रयोगकर्ताको डिजिटल वित्तीय खातामा अनधिकृत पहुँच प्राप्त गर्ने जस्ता घटना भइरहेका छन् र हाम्रो अघिल्लो मिडिया अनुगमन रिपोर्टमा पनि समावेश विषय हो।

यसरी, समग्रमा हेर्दा, टेलिकम र वित्तीय संस्थाहरूको प्रमाणिकरण प्रणालीमा देखिएको कमजोरीले ठगी र डाटा चोरीलाई बढावा दिएको छ। नागरिकता, फोन नम्बर, वा अन्य व्यक्तिगत विवरणहरू चोरी गरी दुरुपयोग गर्नुले व्यक्तिगत गोपनीयताको गम्भीर उल्लङ्घन गर्ने खालको अपराध हो।

४.१.२. बढ्दो साइबर ठगीमा युवाको उल्लेख्य सहभागिता: नेपाल राष्ट्र बैंकको प्रतिवेदन

नेपालमा बढ्दै गएको साइबर ठगी, बैंक तथा वित्तीय संस्थाहरू सहित ई-वालेट प्रणालीका कमजोरीहरू नेपाल राष्ट्र बैंकको एक प्रतिवेदनमा उल्लेख छ। रिपोर्टले सामाजिक सञ्जाल, नक्कली गिफ्ट र पार्सलको लोभ देखाएर ठगी गर्ने र साझा KYC कागजातको दुरुपयोग गरेर बैंक खाता खोल्ने प्रवृत्ति साइबर ठगीका मुख्य कारणका रूपमा देखाएको छ।। ठगीमा अधिकांश युवा संलग्न छन्, विशेष गरी १९-२४ वर्ष उमेर समूहका। नेपालमा साइबर ठगीको समस्या तीव्र रूपमा बढ्दै गएको छ। बैंक तथा ई-वालेट प्रणालीको कमजोरीका कारण व्यक्तिगत डाटाको दुरुपयोग, अनधिकृत खाता पहुँच, र कमजोर सुरक्षा उपायहरूले प्रयोगकर्ताको डिजिटल अधिकार उल्लङ्घन भएको देखिन्छ। यस समस्यालाई नियन्त्रण गर्न बायोमेट्रिक प्रमाणीकरण, मल्टिफ्याक्टर सुरक्षा प्रणाली, र लेनदेन निगरानी प्रणालीको आवश्यकतामा जोड दिइएको छ।

४.१.३. डिजिटल बैंकिंग सेवाभित्र सुरक्षा चिन्ता

नेपालमा डिजिटल बैंकिङ सेवाको सबैभन्दा ठूलो सञ्जाल रहेको F1 Soft International को Citizens International Bank मा रहेको खाताबाट रकम चोरी भएको घटनाले अनलाइन बैंकिङ नेटवर्कमाथि नै थप चिन्ता बढाएको छ। Citizens Bank लगायतका ६९ वटा बैंक तथा वित्तीय संस्थाले F1 Soft कै सिस्टम प्रयोग गर्छन्। यसको अर्थ यदि F1 Soft द्वारा निर्माण गरिएको सिस्टम ह्याक भइ पैसा अन्त ट्रान्सफर हुन सक्छ भने यसले सम्पूर्ण बैंकिङ क्षेत्रकै अनलाइन प्रणाली जोखिममा रहेको संकेत गर्दछ।

४.१.४. सरकारी डिजिटल स्पेसमा गोपनियताको सवाल

गत वर्षजस्तै, यस वर्ष पनि सरकारी डिजिटल स्पेसमा वैयक्तिक गोपनियताको अवस्था परिवर्तनविहीन रह्यो। निर्वाचन आयोगको वेबसाइटमा मतदाता नामावली अझै पनि जो–कोहीलाई खुला रूपमा पनि पहुँच हुने गरी प्रकाशित छ, भने सवारी चालक अनुमतिपत्रको लिखित परीक्षा परिणाम सार्वजनिक रुपमा अनलाइन प्रकाशित हुँदा व्यक्तिको दर्ता नम्बर र नागरिकता नम्बर सहित प्रकाशित हुन्छ।

२०२४ को जून महिनामा यातायात व्यवस्था विभागले लाइसेन्स परीक्षाफलसँगै आवेदकको नागरिकता नम्बर सार्वजनिक नगर्ने भन्ने समाचार आएपनि उक्त अवस्था डिसम्बरसम्म यथावत् रहेको पाइयो।

सञ्चार माध्यममा यसरी नागरिकता नम्बर सार्वजनिक गर्दा सो नम्बर 'निर्वाचन आयोगको वेबसाइटमा रहेको मतदाता नामावलीको सर्चबक्समा राखेर कुनै पनि व्यक्तिको नाम, थर, जन्ममिति, ठेगाना आदि जस्ता अति संवेदनशील जानकारीमा सहजै पहुँच पुर्याईदिन्छ' शिर्षकको समाचार प्रासंगिक देखिन्छ। देखिन्छ।

यसरी, सरकारी निकायहरूबाट नै गोपनीयता भंग हुनुले नागरिकता, वित्तीय विवरण, र अन्य संवेदनशील जानकारीको दुरुपयोगको खतरा बढाएको छ।

प्रतिनिधि घटना/कथा:

ल्यापटप चोरेको मान्छेको नाम, थर र पालिका थाहा भएपछि निर्वाचन आयोगको वेबसाइटमा उपलब्ध मतदाता नामावलीको विवरण झिकेर ल्यापटप धनीले ल्यापटप फिर्ता ल्याए । उनले पुलिसमा जाहेरी गरेपछि, पुलिसले यसमा सहयोग गर्न नसक्ने भएपछि उक्त व्यक्ति यसरी अघि बढेका हुन्।

यो एउटा अपवादको घटना हो, जहाँ आफ्नो ल्यापटप फिर्ता पाउने मनशाय/मोटिभ देखिन्छ ।

समग्रमा, कुनै पनि सार्वजनिक निकाय, विशेषगरी निर्वाचन आयोगको वेबसाइटमा यसरी जो-सुकै व्यक्तिको व्यक्तिगत विवरणमा पहुँच हुनु वैयक्तिक गोपनीयताको हनन हो । साथै, यस्तो प्रणाली रहनु भनेको पहिचान चोरीको जोखिमलाई भयावह बनाउनु मात्र होइन यससम्बन्धी दुर्घटना घटाउनलाई प्रोत्साहन दिनु हो । यसमा सशक्त मिडिया कभरेज र नागरिक समाजका मञ्च तथा सामाजिक वृत्तबाट निर्वाचन आयोगको ध्यानाकर्षण गराउनुपर्छ ।

त्यस्तै, स्थानीय स्थानिय तहका सरकारी वेबसाइटहरूको बारम्बार ह्याकिङले न केवल व्यक्तिगत डाटाको सुरक्षा जोखिम बढाएको छ, तर सरकारी सेवाहरूमा पहुँच पनि अवरुद्ध गरेको छ। नियमित रूपमा बिग्रिने वा राम्रोसँग अपडेट नगरेका असक्षम नगरपालिका वेबसाइटहरूले आधारभूत सार्वजनिक सेवामा ढिलाइ र असुविधा निम्त्याएका छन्।

यी सबै घटनाहरूको मुख्य कारण कमजोर साइबर सुरक्षा पूर्वाधार, तेस्रो पक्ष सेवा प्रदायकहरूमा अत्यधिक निर्भरता, र सुरक्षा उल्लङ्घनपछिको ढिला तथा कमजोर प्रतिक्रिया प्रणाली हो। इन्टरनेट प्रयोगकर्ताका लागि यी समस्याहरूले डिजिटल प्रणालीप्रति विश्वासको ह्रास, गोपनीयताको डर, वित्तीय जोखिम, र सेवामा निरन्तर अवरोधको समस्या निम्त्याएका छन्। हामीले सहजताको लागि डिजिटल सेवाहरूलाई अँगालेका छौँ, तर पछिल्ला घटनाक्रमहरूले अनलाइन प्रणालीको सुरक्षामा गम्भीर प्रश्न उठाउनुका साथै सरकारको डिजिटल उत्तरदायित्वप्रति आलोचना पनि जन्माएको छ।

४.१.५. अन्तर्राष्ट्रिय डिजिटल स्पेसको अवस्था

मेटाले आफ्नो सोशल मिडिया प्लाटर्फमहरु फेसबुक र इन्स्टाग्राममा Link History नामक नयाँ फिचर ल्याएको छ। प्रयोगकर्तालाई लक्षित विज्ञापन (personalised ads) देखाउनका लागि भनिए पनि यसले प्रयोगकर्ताको डाटा थप संकलन गर्छ। प्रयोगकर्ताले यसलाई बन्द पनि गर्न सक्छन् तर एपमा डिफल्ट रुपमा यो फिचर खुल्ला रहेको हुन्छ। प्रविधिमा प्रयोगकर्ताको गोपनियतालाई मजबुत बनाइनुपर्छ भन्ने आवश्यकता रहँदा मेटाले भने प्रयोगकर्ताका डाटा जम्मा गर्नका लागि नयाँ नयाँ तरिकाहरु खोजी रहन्छ। मेटालाई प्रयोगकर्ताका डाटा ट्र्याक गर्ने गरेको आरोप लाग्छ।

अर्को तर्फ, क्रोमको इन्कग्निटो मोडमा पनि डाटा संकलन गर्ने गरेको तर प्रयोगकर्तालाई जानकारी नगराएको गूगलले स्वीकारेको छ। यी दुईजना टेक जाइंट्सले प्रयोगकर्ताको डाटाप्रति संवेदनशील नभएको देखिन्छ। अनलाइन प्रविधिमा प्रयोगकर्ताको गोपनीयताको हक अन्तर्गत, कसरी, कति र कस्तो डाटा कहाँ र कतिको प्रयोग गर्ने अधिकार प्रयोगकर्तासँग हुँदैन। यसमा कम्पनीहरू जवाफदेही हुनुपर्छ।

त्यस्तै अर्को चिन्ताजनक घटना, संसारभरिबाट डाटा लीकका घटना बेलाबेला सुनिएको हुँदा यस वर्ष एउटै ह्याकरबाट करिब 10 अर्ब (९ अर्ब ९४ करोड ८५ लाख ७५ हजार ७३९ युनिक प्लेन टेक्स्ट) पासवर्ड लीक भएको घटना साइबर न्यूजले रिपोर्ट गरेको छ। यसो हुँदा ह्याकरले लिक वा कम्प्रोमाइज भएको पासवर्डहरूको सूची प्रयोग गरेर कुनै सार्वजनिक सिस्टम वा व्यक्तिगत अकाउन्टमा अनाधिकृत पहुँच बनाउँछ। यसलाई क्रेडेन्सियल स्टफिङ पनि भनिन्छ। थप, साइबर न्युजको वेबसाइटमा गएर आफ्नो पासवर्ड लिक भएको/नभएको तथा आफ्नो मोबाइल नम्बर र ईमेल लिक भएको/नभएको यकिन गर्न सकिन्छ।

४.१.६. नेपालमा डीपफेक

हालैका केही घटनाहरूले डिपफेक प्रविधिसँग सम्बन्धित गम्भीर चिन्ताहरू उजागर गरेका छन्, जसले सार्वजनिक व्यक्तिहरूको प्रतिष्ठा र सूचनाको अखण्डतामा असर पुर्‍याएको छ। उदाहरणका लागि, काठमाडौँ महानगरपालिकाका मेयर बालेन शाह र उपमेयर सुनिता डंगोलको डिपफेक भिडियो सामाजिक सञ्जालमा भाइरल भयो, जहाँ उनीहरूलाई चुम्बन गर्दै देखाइएको थियो। उक्त भिडियो डिपफेक प्रविधिको प्रयोगबाट बनाइएको पुष्टि भएपछि सामाजिक सञ्जालमा यसले ठूलो बहस निम्त्यायो। उपमेयर डंगोलले झूठा भिडियोको सिर्जना र वितरणको लागि जवाफदेहीता खोज्दै साइबर ब्युरोमा उजुरी दर्ता गरिन्/गराइन्। यो कदमले व्यक्तिको गोपनीयता र सार्वजनिक विश्वासका लागि डिपफेकहरूको गम्भीर प्रभावलाई दर्शाउँछ, साथै यस्ता मुद्दाहरूलाई प्रभावकारी रूपमा सम्बोधन गर्न कानूनी/नियमनकारी ढाँचाहरूको आवश्यकता पनि देखाउँछ।

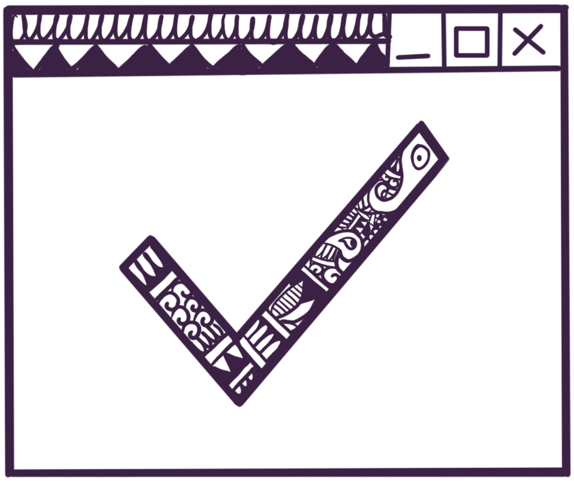
यस्तै, एउटा अर्को घटनामा, २२ वर्षीय व्यक्तिलाई प्रधानमन्त्रीसहितका प्रमुख व्यक्तिहरूको डिपफेक भिडियो बनाएको आरोपमा गिरफ्तार गरियो। यो गिरफ्तारीले डिपफेक प्रविधिको दुरुपयोगसँग सम्बन्धित नियमनको महत्त्वलाई दर्शाउँछ। यसै संदर्भमा, प्रहरीले डिपफेक प्रविधिद्वारा सहजै फैलिने गलत सूचनाबारे चेतावनी जारी गर्‍यो। सम्पूर्ण रूपमा, यी घटनाहरूले डिपफेक प्रविधिको दुरुपयोग विरुद्धको सार्वजनिक जागरूकता र नियामक उपायहरूको तात्कालिक आवश्यकतालाई देखाउँछ। समग्रमा, यी घटनाले डिपफेक प्रविधिबाट हुने सम्भावित हानिबाट जोगिनका लागि कानुनी, प्राविधिक र सामाजिक पहलहरू आवश्यक छन्। यसका लागि राज्य, नागरिक समाज, मिडिया, र डिजिटल अधिकारकर्मीहरू बीच सहकार्य र गहिरो छलफल आवश्यक छ।

४.१.७. नक्कली प्रहरी इमेल ठगी

हरेक वर्षजस्तै, यस वर्ष पनि नयाँ प्रकारको साइबर ठगी देखा परेको छ। यस वर्ष नयाँ प्रकारको साइबर ठगी देखा पर्‍यो, जसमा ठगहरूले प्रहरी अधिकारीको नक्कल गरेर प्रयोगकर्तालाई ठगी गर्ने प्रयास गरे। यो ठगी योजनामा ठगहरूले आधिकारिक जस्तो देखिने इमेलहरू मार्फत व्यक्तिहरूलाई पोर्न सामग्रीमा संलग्न भएको आरोप लगाउँछन्। इमेलमा कानुनी कारबाही, जरिवाना वा पक्राउको धम्की दिइन्छ, जसले पीडितहरूलाई त्रासमा पारेर आर्थिक विवरण उपलब्ध गराउन वा भुक्तानी गर्न बाध्य बनाउने प्रयास गरिन्छ। यस प्रकारको ठगी डर र अन्योलको फाइदा उठाएर चलाइन्छ, जसले गर्दा व्यक्तिहरू सजिलै ठगीको सिकार बन्न सक्छन्। सम्बन्धित निकायहरूले यस्तो ठगीप्रति सचेत रहन आग्रह गर्दै यस्ता इमेलहरूमा प्रतिक्रिया नदिन, कुनै शंकास्पद लिङ्कहरू क्लिक नगर्न, र घटना साइबर सुरक्षा निकायहरूमा रिपोर्ट गर्न सल्लाह दिएका छन्। यस्ता घटनाहरू नेपालमा बढ्दो डिजिटल सुरक्षाका चुनौतीहरूलाई उजागर गर्छन्। यस घटनाले नेपालमा साइबर सुरक्षासम्बन्धी जनचेतना र बलियो डिजिटल सुरक्षा संरचनाको आवश्यकता झनै तीव्र भएको देखाउँछ।

४.२.

‘डिजिटल नेपाल’ का असुरक्षित प्रयासहरु



सरकारी तथा नियमन आवश्यक सेवाहरूमा डिजिटल प्रणालीको विस्तार भइरहेको छ। तर यो विस्तारसँगै प्रयोगकर्ताको व्यक्तिगत जानकारीको सुरक्षा र गोपनीयता सुनिश्चित गर्ने प्रयास भने पर्याप्त देखिँदैन। डिजिटल अधिकार उल्लंघन भएका अवस्थामा नागरिकले सहज रूपमा न्याय पाउने, प्रयोगकर्तामैत्री कानुनी व्यवस्था र संरचना अझै निर्माण भएको छैन।

यसले ‘डिजिटल नेपाल’ अभियानमा सुरक्षाको दृष्टिकोणमा गम्भीर कमजोरी रहेको संकेत गर्दछ।

४.२.१. क्रसबोर्डर डिजिटल भुक्तानी सेवा

यस वर्ष नेपाल र भारतबीच क्रसबोर्डर डिजिटल भुक्तानी सेवा सुरू भयो, जसअनुसार भारतीय प्रयोगकर्ताहरूले नेपालमा सेवा वा सामान खरिद गर्दा भारतीय UPI मार्फत QR स्क्यान गरी भुक्तानी गर्न सक्छन्। त्यस्तै, नेपाली प्रयोगकर्ताहरूले डिजिटल वालेट वा मोबाइल बैंकिङबाट भारतमा QR स्क्यान गरी भुक्तानी गर्न सक्ने व्यवस्था गरिएको छ। यस्तो सुविधाले पारस्परिक लाभ त दिन्छ, तर यससँगै प्रयोगकर्ताको डाटा सुरक्षाबारे गम्भीर प्रश्नहरू पनि उठेका छन्।

नेपालमा बारम्बार साइबर आक्रमण तथा डाटा चोरी हुने गरेका छन्, भने भारतमा पनि आधार कार्डजस्ता संवेदनशील विवरणहरू लिक हुने घटनाहरू सार्वजनिक भएका छन्। अहिले अनलाईनमार्फत वित्तीय ठगी हुने क्रम बढेको छ। क्रसबोर्डर हुने भुक्तानीसँगै साटिने व्यक्तिगत विवरणलाई (खासगरी मोबाइल नं जुन बैंक अकाउन्टसँग लिंक भएको हुन सक्छ) साइबर सुरक्षा प्रदान गर्नुतिर सरोकारवालाको ध्यानाकर्षण हुन जरुरी छ।

४.२.२. राष्ट्रिय परिचयपत्रको उपयोग विस्तार: डिजिटल समावेशिता कि बहिष्करण?

यस वर्ष सरकारले राष्ट्रिय परिचयपत्रलाई राज्यले प्रदान गर्ने सेवासँग आबद्ध गर्ने भन्यो। साथै, राष्ट्रिय परिचयपत्रलाई सरकारी पहिचान पत्रको रुपमा विकास गर्दै बैंक खाता खोल्न, ड्राईभिंग लाइसेन्स फारम भर्न, ब्लुबुक , प्यान आदिका लागि अनिवार्य बनाउने योजना सार्यो। स्मार्टकार्ड छाप्नु नपर्ने गरी ड्राईभिंग लाइसेंसको काम पनि राष्ट्रिय परिचपत्रले गर्ने भनियो। मूलत: सरकारले राष्ट्रिय परिचयपत्र सिम कार्ड निकाल्न, बैंक खाता खोल्न र सामाजिक सुरक्षा भत्ता पाउन लगायतका सार्वजनिक सेवा प्रवाहमा अनिवार्य गर्ने जस्ता उपयोगिता विस्तारका प्रयासहरु थाल्यो। यद्यपि, यसले सबै नागरिकलाई समान पहुँच उपलब्ध गराउने सुनिश्चित गर्दैन।

सीमान्तीकरणमा रहेका समुदायहरू जस्तै महिला, दलित, आदिवासी, र LGBTQIA+ समुदायका व्यक्तिहरू आवश्यक कागजातको अभावमा राष्ट्रिय परिचयपत्र प्राप्त गर्न संघर्षरत छन्। यस्तो अवस्थामा उनीहरू सरकारी सेवा, बैंकिङ प्रणाली, र डिजिटल पहुँचबाट वञ्चित हुने खतरा बढ्दो छ। नागरिकता नभएका वा प्रक्रिया पूरा गर्न नसकेका व्यक्तिहरू त झन् यो प्रणालीबाट पूर्णरूपमा बहिष्कृत हुने खतरा सामना गर्छन्, जसले डिजिटल डिभाइडलाई अझ गहिरो बनाउँछ।

अर्को तर्फ, एकीकृत पहिचान पत्रको अवधारणालाई बल दिन त्यसो गरिएको भनिएता पनि सरकारी डाटाबेस माथिको हालसालै दोहोरिएका साईबर हमलाहरुले सरकार नागरिकको डाटा सुरक्षामा चुकेको देखिन्छ। न त नागरिकले बायोमेट्रिक डाटालगायत कतिसम्मको वैयक्तिक जानकारी सरकारलाई साझा गर्ने सम्बन्धी स्पष्ट कानुनी व्यवस्था छ — जसको अभावमा महिला अधिकारकर्मी, पत्रकार, र LGBTQIA+ समुदायमाथि निगरानीको जोखिम उत्पन्न हुन सक्छ। त्यसरी साझा गरिएको जानकारी सरकारले के-कस्तो प्रयोजनको लागि चलाउन मिल्ने र नमिल्ने, वा चलाएमा नागरिकको गोपनियता सुरक्षित पार्न के गर्ने (?) सरकारले नागरिकमैत्री नीति बनाउनुपर्ने हुन्छ।

यस अतिरिक्त, सहजताका लागि वडाबाट नै राष्ट्रिय परिचयपत्रको आवेदन दिन मिल्ने भनिए पनि यदि त्यहाँ वैयक्तिक जानकारी गलत टाइप हुन्छ भने त्यसलाई सच्याउन जिल्ला प्रसाशन कार्यालय नै पुग्नुपर्ने बाध्यता रहेको छ। जसले गर्दा जिल्ला सदरमुकामबाट बाहिर वा टाढा बस्ने व्यक्तिका निम्ति राष्ट्रिय परिचयपत्र पहुँच योग्य हुन सकेको छैन।

यस वर्षको उतरार्धमा राष्ट्रिय परिचयपत्रलाई नागरिक एपसँग आबद्ध गरियो। तर नागरिक एपमा देखिएको पिन कोड बाइपास हुने बगले गर्दा त्यहाँ रहेको संवेदनशील वैयक्तिक जानकारी लिक हुने जोखिम देखियो। त्यस्तै, सर्भरमा मालवेर छिरेपछि राहदानी सेवा पाँच दिनसम्म अवरुद्ध रह्यो भने नेपाल राष्ट्र बैंकलगायत थुप्रै सरकारी वेबसाइट डाउन भए। यस वर्षभरि मात्रै नभएर अघिल्ला वर्षहरुमा समेत विभिन्न सरकारी वेबसाइटहरुमा भएका साइबर आक्रमण सामान्य जसो भैसकेको बुझिन्छ।

यस्ता प्रकरणहरूले के देखाउँछन् भने न नेपालमा डिजिटल पूर्वाधार पर्याप्त सुरक्षित छन्, न त नागरिकको अधिकार सुरक्षित गर्न कानुनी संरचना मजबुत छ।

४.२.३. प्रविधिमा अपाङ्गता भएका व्यक्ति बहिष्करणमा

डिजिटाइजेसनका नाममा आधारभूत सेवाहरूमा पहुँच विस्तार गर्ने भनिए पनि ती प्रयासहरू सबैका लागि समान रूपले पहुँचयोग्य छैनन्। बैंकिङजस्ता सेवा प्रणालीमा अपाङ्गता भएका व्यक्तिहरू, विशेषत: दृष्टिविहिनहरू, अझै पनि बहिष्करणको शिकार भइरहेका छन्।

नेपालमा दृष्टिविहिन व्यक्तिहरूले डिजिटल बैंकिङ सेवा प्रयोग गर्न निकै संघर्ष गर्नुपर्छ। बैंकहरूले "वित्तीय सुरक्षाका कारण" वा "आन्तरिक नीतिका आधारमा" दृष्टिविहिन व्यक्तिले एक जना आँखा देख्ने साक्षीको उपस्थितिमा मात्र बैंक खाता खोल्न पाउने जस्ता प्रावधान लागू गरिरहेका छन्। यस्तो नीति स्वयं अपमानजनक, अपाङ्गता भएकाप्रति अविश्वास दर्शाउने र उनीहरूलाई पूर्ण नागरिकको रूपमा नस्वीकार्ने व्यवहारको प्रतिबिम्ब हो।

आजको प्रविधिमा, ब्रेल लिपि, स्क्रिन रिडर सफ्टवेयर, र मोबाइल चलाउने दृष्टिविहिन मैत्री प्रविधिहरू सहज रूपमा उपलब्ध छन्। तर बैंकिङ प्रणालीले यी प्रविधिलाई आत्मसात नगर्नु, र दृष्टिविहिन व्यक्तिहरूलाई अझै पनि अरूको सहयोगमा सेवा लिन बाध्य बनाउनु, डिजिटल बहिष्करण को स्पष्ट उदाहरण हो। यस्तो बहिष्करणले दृष्टिविहिन नागरिकलाई आत्मनिर्भर हुन दिँदैन, उनीहरूलाई झनै सीमान्तीकरणको स्थितिमा पुर्‍याउँछ। डिजिटल समावेशिताका नाममा गरिने प्रयासहरू अपाङ्गता भएका व्यक्तिहरूका लागि व्यवहारमै समान पहुँच सुनिश्चित गर्नतर्फ उन्मुख हुनुपर्छ। डिजिटल बैंकिङ सेवा, मोबाइल एप, अनलाइन सेवा प्रणालीहरू — यी सबै दृष्टिविहिन र अन्य अपाङ्गता भएका व्यक्तिहरूका लागि पहुँचयोग्य बन्नु अत्यावश्यक छ। यसका लागि नीतिगत सुधार, प्रविधि समायोजन, र सेवा प्रदायकहरूको सम्वेदनशीलता वृद्धि अनिवार्य छ।

४.२.४. नक्कली चालक अनुमतिपत्र प्रकरण: डिजिटल अधिकार र गोपनीयताको चुनौती

नेपालमा सार्वजनिक सेवा वितरणसँग जोडिएको अनियमितता र भ्रष्टाचार अब प्रविधिमार्फत पनि देखिन थालेको छ, जसको ताजा उदाहरण नक्कली चालक अनुमतिपत्र वितरण प्रकरण हो। पाँच जना सरकारी कर्मचारी पक्राउ परेको यस घटनाले व्यक्तिगत डाटा दुरुपयोग, डिजिटल अभिलेख प्रणालीको असुरक्षा, र प्रशासनिक प्रक्रियामा पारदर्शिताको अभावलाई उजागर गरेको छ। डिजिटल प्रणाली प्रयोग गरेर जारी गरिने सरकारी प्रमाणपत्रहरूमा यस्ता अनियमितता हुनु भनेको प्रयोगकर्ताको डिजिटल अधिकार र गोपनीयता गम्भीर रूपमा प्रभावित हुनु हो।

यस प्रक्रियामा सेवाग्राहीको व्यक्तिगत जानकारीहरू गलत तरिकाले प्रयोग गरिए, वा डाटाबेस नै ह्याक/बाइपास गरियो भन्ने सम्भावनाले डाटा सुरक्षाको गम्भीर

प्रश्न उठाएको छ। यदि सरकारी डिजिटल प्रणाली नै कमजोर वा अनियमिततायुक्त छ भने, व्यक्तिगत जानकारीहरू चोरी, दुरुपयोग, वा अवैध कारोबारको जोखिममा पर्ने सम्भावना उच्च हुन्छ। यसले डिजिटल प्रशासनमा विश्वासको संकट सिर्जना गर्न सक्छ।

यस घटनाले नेपालमा डिजिटल प्रणालीमा हुने डाटा सुरक्षा उल्लंघन, साइबर जोखिम, र व्यक्तिगत जानकारीको दुरुपयोगलाई रोक्न सुधारका उपायहरू अवलम्बन गर्नुपर्ने आवश्यकता देखाएको छ। डिजिटल अधिकारको रक्षा, नागरिकको गोपनीयता सुनिश्चित गर्ने प्रभावकारी साइबर सुरक्षा नीति, र सबल डिजिटल अभिलेख प्रणाली अब केवल विकल्प होइन, अनिवार्य आवश्यकता हो।

४.३. प्रविधिमा आधारित हिंसा

यस वर्ष महिलाविरुद्ध प्रविधिमा आधारित हिंसा (अनलाईन भायलेन्स) प्रायः रिभेन्ज पोर्नको रूपमा देखा पर्यो भने नेपाल प्रिमियर लिगको सन्दर्भमा मधेसी समुदायविरुद्ध अनलाइन गरिएको नश्लीय द्वेषपछि शारीरक हिंसामा परिणत भयो। LGBTQIA+ समुदायले सामाजिक सञ्जालमा विभेद भोग्दै छ।

प्रविधिमा आधारित हिंसाका यस्ता घटनाहरूले डिजिटल प्लेटफर्महरूमा पर्याप्त नियमनको अभाव, पीडितका लागि प्रभावकारी सहायता प्रणालीको कमजोर अवस्था, र साइबर अपराधप्रति संस्थागत संवेदनशीलताको कमीलाई उजागर गर्छन्। विशेषगरी सामाजिक सञ्जालमा हुने ट्रोलिङ, अभद्र टिप्पणी, धम्की, वा निजी सामग्रीको दुरुपयोगले सीमान्तकृत समुदायहरूलाई अझ असुरक्षित बनाएको छ।

यस सन्दर्भमा राज्य र डिजिटल सेवा प्रदायकहरूले प्रविधिमा आधारित हिंसाविरुद्ध स्पष्ट नीति, शीघ्र कारबाही प्रणाली, तथा पीडितमैत्री सहायता संयन्त्र निर्माण गर्नुपर्ने आवश्यक देखिन्छ।

४.३.१. महिलाविरुद्ध रिभेन्ज पोर्न

महिलाविरुद्ध प्रविधिमा आधारित हिंसा (अनलाईन भायलेन्सका) एकै खाले केही घटनाहरू जून महिनामा रिपोर्ट भयो। एकआपसको सहमतिमा दुई वयशक व्यक्ति — एक महिला र एक पुरुष (consenting adults — a woman and a man) बीचको इन्टीमेट क्षणको खिचिएको फोटो तथा भिडियोलाई पुरुषले महिलालाई [बिना सहमति] विभिन्न स्वार्थपूर्तिको लागि **ब्ल्याकमेल गर्न, चरित्र हत्या गर्न** र मानसिक तनाब दिन सामाजिक सञ्जालमा सार्वजनिक गरेको पाइन्छ । **सम्बन्धमा खटपट परेपछि** पुरुषले ईख मानेर प्रतिशोधको रूपमा उक्त फोटो र भिडियो सार्वजनिक गरिदिने परिपाटी देखिन्छ । यस परिपाटीलाई रिभेन्ज पोर्न भनिन्छ । पुलिसको तथ्यांकले पनि **महिलाविरुद्ध प्रविधिमा आधारित हिंसा बढेको** देखाउँछ । यद्यपि रिभेन्ज पोर्न' भनेर छुट्टै श्रेणीमा वर्गीकरण गरिएको छैन। (प्रहरी तथ्यांकबारे थप जानकारी मिडिया अनुगमन वार्षिक प्रतिवेदन, २०२३, पृष्ठ १७ मा हेर्न सकिन्छ।)

त्यस्तै, रिभेन्ज पोर्न तथा यसै वरिपरी अन्य प्रकृतिका अनलाईन हिंसाका घटनाहरु पनि रिपोर्ट भएका छन्। अधिकांश घटनाहरु महिलाविरुद्धका छन्। प्रायः घटनाहरुमा **रिस** वा **ब्ल्याकमेल** गर्ने उद्देश्यले पीडितको फोटो र भिडियो एडिट गरेर वा **लुकीछिपी खिचेर** त्यसलाई पोर्नोग्रफिक कन्टेन्ट बनाइ इन्टरनेटमा सम्प्रेषण गरिन्छ। थपमा, कुनै तेस्रो व्यक्तिले दुई जना बीचको **गोप्य क्षणको फोटो र भिडियो सामग्रीमा अनाधिकृत पहुँच पुर्याएर** ती दुई जनाको सहमति बिना आफन्तमाँझ वा इन्टरनेटमा सार्वजनिक गरेको पनि पाइन्छ। यस्तो ट्रेन्ड प्रायः किशोरकिशोरी उमेर समूहको प्रेम सम्बन्धमा देखिन्छ। यस्तै, २०८० सालको एउटा **अनलाइन ह्यारेसमेन्ट**सम्बन्धी घटनामा यसै महिना अदालतबाट फैसला प्रमाणीकरण भएको छ। उक्त घटनामा एक महिलाले पुरुषको प्रेम प्रस्ताव अस्वीकृत गरेपछि ती पुरुषले बारम्बार मोबाइल नम्बर र इन्स्टाग्राममार्फत सम्पर्क गर्ने, ब्लक गरेपछि इमेल पठाउने जस्ता कार्य गरेका थिए।

४.३.२. मधेसी समुदायविरुद्ध नश्लीय द्वेष

नेपालमा अनलाइन मञ्चहरू, विशेषगरी सामाजिक सञ्जाल, मधेसी समुदायविरुद्ध कुनै न कुनै बहानामा नश्लीय विभेद र घृणाद्वेष फैलाउने माध्यम बनिरहेका छन्। नेपाल प्रिमियर लिगभरि **नश्लीय अपमान**, भ्रामक प्रचार, र घृणास्पद टिप्पणीहरूले डिजिटल मञ्चलाई विषाक्त बनाउँदै सामाजिक एकता खण्डित गरिरहे।

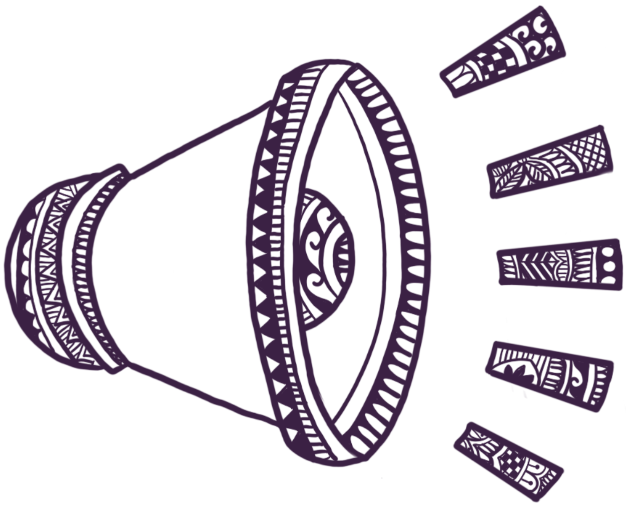
यस समस्याको मूल कारण कमजोर कानुनी कार्यान्वयन, नियमनको अभाव, र प्रयोगकर्तामा डिजिटल चेतनाको कमी हो। कानुनी प्रावधानहरू कमजोर हुँदा घृणास्पद सामग्रीको प्रकाशन र प्रसार सजिलै हुने अवस्था रहेको छ।यसले मधेसी समुदायका इन्टरनेट प्रयोगकर्तामा असुरक्षा र मानसिक तनाव

अझै बढाइरहेको छ। समस्या समाधानका लागि कडा कानुनी कार्यान्वयन, घृणास्पद सामग्री हटाउने प्रभावकारी प्रणाली, र डिजिटल चेतना अभिवृद्धिका अभियानहरू अनिवार्य देखिन्छन्। अनलाइन मञ्चहरू संवाद र सहकार्यका लागि हुनुपर्छ । विभाजन र घृणा फैलाउन मात्र नभइ , सबै पक्षको सहकार्यबिना यो समस्या समाधान हुन सक्दैन। सरकार, डिजिटल प्लेटफर्महरू, र प्रयोगकर्ताहरूले **जिम्मेवारीपूर्वक** कदम चाल्न आवश्यक छ।

४.३.३. LGBTQIA+ समुदायविरुद्ध सामाजिक सञ्जालमा नकारात्मक प्रतिक्रिया

LGBTQIA+ समुदायले **सामाजिक सञ्जालमा नकारात्मक प्रतिक्रिया**को कारण व्यापक भेदभाव र मानसिक दबाबको सामना गरिरहेको छ। यसले उनीहरूलाई विचार र पहिचान खुलाएर प्रस्तुत गर्न झनै कठिन बनाइरहेको छ।। समुदायका सदस्यहरू सामाजिक सञ्जालमार्फत जागरूकता फैलाउने कोसिस गर्दा पनि नकारात्मक कमेन्टले उनीहरूलाई निरुत्साहित गरिरहेको देखिन्छ। यसले समाजमा गहिरो रूपमा गढेको पूर्वाग्रह र असहिष्णुतालाई उजागर गर्छ।

४. ४.
वाक स्वतन्त्रता



४.४.१. सीधाकुराको स्टिङ अपरेसन र अदालतको कारबाही

यस अप्रिल सीधाकुरा भन्ने युट्युब च्यानलमा प्रकाशित कथित अदालती भ्रष्टाचारबारे कथित स्टिङ अपरेसन गरेको अडियो सार्वजनिक भयो। सर्वोच्च अदालतले तुरुन्तै (जसलाई अस्वाभाविक मानिँदै छ) सुओ मोटो कोग्नीजेन्स (संज्ञान लिनु) लिँदै अदालतको अवहेलना अन्तर्गत सो अडियो हटाउन निर्देश दिएको थियो र उक्त च्यानल सञ्चालक(हरु)माथि फौजदारी कारबाही गर्न आदेश दियो।

यस घटनासँग सम्बन्धित रूपमा, पत्रकार महासंघले सर्वोच्च अदालतले बिना छानबिन अडियो हटाउने र फौजदारी मुद्दा नै चलाउने आदेश दिएको विषयमा प्रेस/वाक स्वतन्त्रताविरुद्ध हुने आशयको प्रेस विज्ञप्ति निकालेको थियो।

यो केसमा अदालतको मानमर्दन हुन नदिन र न्यायप्रति जनविश्वास गुम्न नदिन अदालतले यस्तो कदम चालेको भनिए तापनि, अदालत पनि राज्यको अंग भएकाले, यस्ता कदमले गलत नजिर बस्न सक्ने जोखिम रहन्छ।

४.४.२. टिकटक माथिको प्रतिबन्ध हटाइनु: डिजिटल स्वतन्त्रता कि नियन्त्रण?

नेपाल सरकारले नोभेम्बर २०२३ मा सामाजिक सद्भाव बिगारेको कारण देखाउँदै टिकटकमाथि प्रतिबन्ध लगायो। तर अगस्ट २०२४ मा सरकारसँग सम्झौता गरेपछि उक्त प्लेटफर्मलाई पुनः सञ्चालनको अनुमति दिइयो। त्यसपछि, टिकटक नेपालमा दर्ता भयो र सम्झौताअनुसार एउटा 'फोकल पर्सन' नियुक्त गर्यो। सम्झौतामा सरकारले नयाँ सामग्री हटाउने प्रणाली र सरकारी निगरानीको स्वीकृतिलगायत अनुगमन बढाउने शर्त समावेश थिए।

यस कुराले डिजिटल अधिकारहरूमा महत्वपूर्ण प्रभाव पार्ने अवस्था सिर्जना गर्छ। एकातिर, कानुनी इकाइको रूपमा दर्ता भएपछि, टिकटकले आफ्नो कार्यमा जवाफदेहीता र पारदर्शिता बढाउन सक्छ, जसले डाटा गोपनीयता र सामग्री व्यवस्थापनमा सुधार ल्याउन सक्ने अपेक्षा गर्न सकिन्छ। प्रयोगकर्ताहरूको गोपनीयता, सुरक्षा, र हानिकारक सामग्रीबारे छिटो प्रतिक्रिया दिन सहजता आउन सक्छ। त्यस्तै, प्रयोगकर्ताहरूले आफ्नो चासो र समस्याबारे आवाज उठाउन सक्ने, र समाधान खोज्न सक्ने वातावरण बन्न सक्छ, जसले उनीहरूको अधिकार सशक्त बनाउँछ र डिजिटल क्षेत्रमै उनीहरूको हकहित सुनिश्चित गर्छ।

तर, कानुनी इकाइको रूपमा टिकटक दर्ता भएपछि, सरकारले प्रयोगकर्ताको अभिव्यक्ति स्वतन्त्रतामाथि सिधै निगरानी राख्न सक्ने, र राजनैतिक स्वार्थ पूरा गर्न व्यक्तिगत जानकारीमा पहुँच गर्न सक्ने शंका उत्पन्न हुन्छ। यस्तो कदमले राज्यद्वारा जनतामाथि निगरानीलाई प्रश्रय दिन सक्छ, र झनै सीमान्तकृत समुदायहरू प्रभावित हुन सक्छन्, विशेषतः जसको अभिव्यक्तिले वर्तमान राजनैतिक वा सामाजिक संरचना प्रश्नमा ल्याउँछ।

खासगरी, क्वेयर समुदायप्रतिको सामाजिक पूर्वाग्रहले गर्दा, उनीहरूले टिकटकमार्फत पाएको अभिव्यक्ति स्वतन्त्रता समाजले सहजै पचाउन सक्दैन। त्यसैले, टिकटकमाथिको प्रतिबन्ध हटाइएपछि अब सरोकारवालाहरूले यस प्लेटफर्मलाई सीमित कुलीन वर्गको हतियार बन्न नदिन ध्यान दिनु आवश्यक छ।

उदाहरणका लागि, टिकटकले कम्युनिटी गाइडलाइन्सको उल्लङ्घन — 'भ्रमपूर्ण जानकारी', 'आपत्तिजनक सामग्री', 'घृणास्पद भाषा', र 'साइबर अपराधसँग सम्बन्धित गतिविधि' — भन्दै ६,०७८ भिडियो सामाग्रीहरू हटायो। जसमध्ये ९९.१% सामाग्री रिपोर्ट गरिएको तुरुन्तै हटाइयो भने ९३.२% सामाग्रीहरू २४ घण्टाभित्र हटाइए। यसले अभिव्यक्ति स्वतन्त्रताको सन्दर्भमा गम्भीर प्रश्न उठाउँछ। यसै बेला नेपाल प्रिमियर लिगको पृष्ठभूमिमा मधेसी समुदायविरुद्ध सामजिक सञ्जाल हुँदै शारीरिक रुपमै भएका नश्लीय हमलाका विभिन्न घटनाहरु भिडियो मार्फत टिकटकबाट नै पहिलो पटक पोस्ट भएको देखिन्थ्यो। यस घटनालाई अतः दबाइयो। फलतः यस घटनामा कुनै ठोस कारवाही भएको पाइएन।

यहाँ मुख्य प्रश्न उठ्छ — टिकटकको सरकारसँगको सम्झौता नियमनका लागि हो कि सेन्सरसिपका लागि? प्रतिबन्ध हटाइएको भए पनि, सरकारका सर्तअनुसार टिकटकले स्वतन्त्र विचारलाई सीमित गर्ने नीति अपनाएको देखिन्छ।

४.४.३. गिग अर्थतन्त्र: कन्टेन्ट क्रिएसन

नयाँ पुस्ताले ब्लग लेखन, भिडियो निर्माण, सामाजिक सञ्जालमार्फत जनचेतना फैलाउने र आफ्ना विचारहरू सार्वजनिक गर्ने कार्यमा उल्लेखनीय रुचि देखाइरहेका छन्, जसले डिजिटल प्लेटफर्महरूलाई केवल मनोरञ्जन र जानकारी आदानप्रदानको माध्यम मात्र नभई प्रत्यक्ष आम्दानीको स्रोतसमेत बनाइदिएको छ। यो प्रवृत्तिले डिजिटल अधिकारको सन्दर्भमा बौद्धिक सम्पत्तिको सुरक्षा, कन्टेन्ट क्रिएटरहरूको उचित पारिश्रमिक, र अनलाइन स्वतन्त्र अभिव्यक्ति सुनिश्चित गर्नुपर्ने आवश्यकता झनै स्पष्ट पार्दछ।

तर, यिनै स्पेसभित्र एल्गोरिद्मिक पक्षपात, सामग्री हटाउने अपारदर्शी नीतिहरू, र श्रमको मूल्यांकनमा असमानता जस्ता समस्या पनि उब्जिएका छन्। यस सन्दर्भमा, कडा कानुनी कार्यान्वयन, घृणास्पद र विभाजनकारी सामग्री हटाउने प्रभावकारी प्रणाली, र डिजिटल चेतनामा वृद्धि गर्ने अभियानहरू अनिवार्य बन्न पुगेका छन्। डिजिटल स्पेस संवाद, विविधता र सहकार्यको माध्यम हुनुपर्छ, विभाजन, दमन र घृणाको होइन। यस्तो सुनिश्चित गर्नका लागि सरकार, डिजिटल प्लेटफर्महरू, र प्रयोगकर्ताहरू सबैले आ–आफ्नो भूमिका जिम्मेवारीपूर्वक निर्वाह गर्नु आवश्यक छ। सीमान्तकृत समुदायहरू, विशेषगरी दलित र क्वेयर कन्टेन्ट क्रिएटरहरूका लागि सुरक्षित डिजिटल वातावरण निर्माण गर्नु अहिलेको डिजिटल युगमा गम्भीर प्राथमिकता हुनुपर्छ, जुन सहानुभूतिशील कानुनी संरचना र न्यायोचित एल्गोरिदमिक प्रणालीद्वारा मात्र सम्भव छ।

५ ट्रेन्ड, सिफारिसहरू, र निष्कर्ष

नेपालमा पछिल्लो समय डिजिटल प्रविधिको पहुँच र विस्तार उल्लेखनीय रूपमा बढिरहेको भए तापनि, यसको नियमन र सुरक्षा संरचना अझै पनि कमजोर र सुस्त देखिन्छ। प्रविधि तीव्र गतिमा अघि बढिरहेको बेला नीति निर्माण, साइबर सुरक्षा, र प्रयोगकर्ताको अधिकार संरक्षणको पक्षमा राज्यको तयारी पछि परेको छ। सरकारी डिजिटल प्रणालीहरू बारम्बार साइबर आक्रमणको शिकार भइरहेका छन्, यद्यपि अघिल्ला वर्षहरूको तुलनामा यस वर्ष केही हदसम्म द्रुत रिकभरी देखिएको छ। तथापि, व्यक्तिगत डाटा कत्तिको सुरक्षित रह्यो भन्ने प्रश्नमा सरकार स्वयंले अडिट गर्न आवश्यक छ।

यसैबीच, डिजिटल स्पेस महिलाहरू, अल्पसंख्यक जातीय समुदायहरू, र LGBTQIA+ व्यक्तिहरूका लागि झनै असुरक्षित बन्दै गएको देखिन्छ। प्रविधिको प्रयोगबाट अवसरहरू खुले पनि प्रविधिमा आधारित हिंसा, भेदभाव, र डिजिटल श्रमको शोषण झनै तीव्र रूपमा बढिरहेको छ। राज्य नियमनभन्दा बढी निगरानी र नियन्त्रणमुखी भइदिएकोले अभिव्यक्ति स्वतन्त्रता जस्ता आधारभूत अधिकारहरूमा प्रभाव परेको छ।

विषयगत अवलोकनहरुलाई थप विश्लेषण गर्दा निष्कर्ष र सिफारिसहरु यस प्रकार छन्।

गोपनीयता र डाटा संरक्षण/अनलाइन सेक्युरिटी

नेपालमा साइबर अपराध, डाटा दुरुपयोग, र डिजिटल ठगीका घटनाहरू तीव्र गतिमा वृद्धि भइरहेको सन्दर्भमा, प्रयोगकर्ताको गोपनीयता गम्भीर जोखिममा परेको छ। डिजिटल प्रविधिको विस्तारसँगै व्यक्तिको व्यक्तिगत जानकारी असुरक्षित बन्न थालेको छ, जसले गर्दा बायोमेट्रिक प्रमाणीकरण, मल्टिफ्याक्टर सुरक्षा प्रणाली, र डिजिटल साक्षरताको अभिवृद्धि अपरिहार्य भएको देखिन्छ। डाटा सुरक्षाका लागि प्रभावकारी नीति निर्माण गर्नुका साथै सरकारी तथा निजी संस्थाहरूले आफ्ना कर्मचारीहरूको पृष्ठभूमि जाँच कडा पार्नुपर्छ, गोप्य जानकारीमा पहुँच सीमित राख्नु पर्दछ, र निगरानी प्रविधिको विवेकपूर्ण तथा जिम्मेवार प्रयोग गर्न आवश्यक छ।

साथै, साइबर सुरक्षासम्बन्धी नियमित तालिम तथा अभ्यास कार्यक्रम सञ्चालन गरी प्रणालीगत सुधार ल्याइनु पर्नेछ। साइबर अपराधको सन्दर्भमा पीडितमैत्री कानुनी प्रक्रिया सुनिश्चित गर्नु, छिटो कारबाही गर्न सक्ने संयन्त्र निर्माण गर्नु, र नागरिकलाई कानुनी उपायहरूको जानकारी दिनु पनि अत्यावश्यक छ। डिजिटल रुपान्तरणको यो चरणमा नेपालले प्रविधिको सुरक्षित, समावेशी र उत्तरदायी प्रयोग सुनिश्चित नगर्ने हो भने डिजिटल असमानता अझै गहिरिँदै जान सक्छ। यसैले, सरकार, निजी क्षेत्र, र नागरिक समाजबीचको सहकार्य अपरिहार्य रहेको छ।

डिजिटल नेपाल/ई-गभरनेन्स

नेपालको डिजिटाइजेसनले वित्तीय पहुँच, सेवा सहजता, र सरकारी कार्यप्रणालीमा पारदर्शिता ल्याउने काममा उल्लेखनीय भूमिका खेलेको छ, तर यससँगै डेटा सुरक्षा, गोपनीयता, र समावेशी पहुँचको विषयमा गम्भीर चुनौतीहरू देखा परेका छन्। क्रसबोर्डर भुक्तानी प्रणाली, डिजिटल राष्ट्रिय परिचयपत्र, अपाङ्गता भएका व्यक्तिहरूको डिजिटल पहुँच सुनिश्चित गर्ने उपाय, र सरकारी डिजिटल प्रणालीहरूको प्राविधिक असुरक्षाले यस क्षेत्रका खतराहरूलाई झनै स्पष्ट बनाएको छ। यस्तो अवस्थामा सबै डिजिटल सेवा प्रदायक संस्थाहरूले कडा साइबर सुरक्षा मापदण्ड अनिवार्य रूपमा लागू गर्नुपर्छ, सुरक्षासम्बन्धी उल्लङ्घनहरूको तत्काल जानकारी दिनु आवश्यक छ, र प्रयोगकर्ताहरूलाई नियमित रूपमा अनलाइन सुरक्षा तथा डेटा गोपनीयताको सम्बन्धमा सचेत गराइनु पर्दछ।

यस्तै, कडा डाटा संरक्षण कानून कार्यान्वयन नगरी डिजिटल प्रणालीमा विश्वास कायम राख्न सकिंदैन। जबसम्म सरकारी र निजी संस्थाहरूले साइबर सुरक्षा पूर्वाधारलाई सुदृढ गर्दै यसलाई नीति र कार्यान्वयन दुवै तहमा प्राथमिकता दिँदैनन्, तबसम्म प्रत्येक अनलाइन गतिविधि, लग-इनदेखि भुक्तानीसम्म, प्रयोगकर्ताका लागि जोखिमपूर्ण बन्नेछ। डिजिटल नेपालको परिकल्पनालाई सुरक्षित, समावेशी र विश्वसनीय बनाउन सबै पक्षको सहकार्य अपरिहार्य छ।

प्रविधिमा आधारित हिंसा

नेपालमा प्रविधिमा आधारित हिंसा (अनलाइन भायलेन्स) एक गम्भीर समस्या बनेको छ, जसले विशेष गरी महिलाहरू, मधेसी समुदाय, र LGBTQIA+ समुदायलाई लक्षित गर्दै सामाजिक र मानसिक दबाब सिर्जना गरिरहेको छ। प्रविधिको सकारात्मक पक्ष भनेको यसले विभिन्न अवसरहरू सिर्जना गरेको हो, तर यसको दुरुपयोगले यसका असुरक्षित पक्षलाई उजागर गरेको छ। अनलाइन हिंसा, उत्पीडन, भेदभाव र ट्रोलिंग जस्ता घटनाहरू तीव्र रूपमा वृद्धि भएको छ, जसले मानसिक स्वास्थ्य र सामाजिक समावेशीकरणमा गम्भीर असर पारिरहेको छ। यसबाट स्पष्ट छ कि प्रविधिको पहुँच र प्रयोग सीमान्तीकृत समुदायका लागि अझै सुरक्षित छैन। यस्तो हिंसाका कारण सामाजिक असमानता र भेदभावलाई थप गहिरो बनाउने खतरा छ। यो देखाउँछ कि प्रविधिको सही र सुरक्षित प्रयोगको लागि कानूनी र सामाजिक संरचनामा सुधार आवश्यक छ, ताकि सबै समुदायका लागि समान र सुरक्षित डिजिटल वातावरण सुनिश्चित गर्न सकिन्छ।

वाक स्वतन्त्रता

नेपालमा वाक तथा डिजिटल स्वतन्त्रता अहिले नियमन र नियन्त्रणको दोधारमा रहेको छ। राज्यको हस्तक्षेप प्रेस र डिजिटल स्वतन्त्रतामा बढ्दै गएको छ, जसले नागरिक अधिकार र लोकतान्त्रिक प्रक्रिया सम्बन्धी गम्भीर प्रश्न उठाउँछ। नेपालमा टिकटकको प्रतिबन्ध हटाउनु डिजिटल अधिकारको दृष्टिकोणले मिश्रित संकेत हो। एकातर्फ, प्रयोगकर्ताले पुनः प्लेटफर्ममा पहुँच पाएका छन्, तर अर्कोतर्फ, सरकारी नियन्त्रणमा वृद्धि भएको देखिन्छ। हटाइएका सामग्रीहरूको प्रकारलाई हेर्दा सेन्सरसिपको असमान प्रभाव स्पष्ट देखिन्छ, जसले महिला, मधेसी, दलित, र LGBTQIA+ जस्ता सिमान्तकृत समुदायलाई विशेष गरी प्रभावित गरिरहेको छ। यस्तो सेन्सरसिप र डिजिटल स्वतन्त्रता सीमित गर्ने प्रयासले अल्पसंख्यक र सीमान्तकृत समुदायहरूलाई अझै बढी दबाबमा पार्न सक्छ, जसले नेपालको लोकतान्त्रिक मूल्य र अभिव्यक्ति स्वतन्त्रताको रक्षामा गम्भीर चुनौती पुर्याउन सक्छ।

गिग अर्थतन्त्र: कन्टेन्ट क्रिएसन

गिग अर्थतन्त्रमा कन्टेन्ट क्रिएसन एक महत्वपूर्ण क्षेत्रका रूपमा विकसित भइरहेको छ, जसले नयाँ पुस्तालाई डिजिटल प्लेटफर्महरूमार्फत ब्लग लेखन, भिडियो उत्पादन, र अन्य सामग्री सिर्जनाबाट प्रत्यक्ष आम्दानी गर्ने अवसर प्रदान गरेको छ। यसले सृजनात्मकता र डिजिटल युगमा रोजगारका नयाँ ढोका खोलिदिएको छ। तर, यससँगै बौद्धिक सम्पत्ति अधिकार, उचित पारिश्रमिक, र अभिव्यक्ति स्वतन्त्रतासँग सम्बन्धित विभिन्न चुनौतीहरू पनि देखा परिरहेका छन्। कन्टेन्ट क्रिएटर्सले आफ्नो कामको उचित मुआवजा नपाउने, क्रिएटेड सामग्रीको अधिकारको संरक्षण नहुने, र थाहा नपाएर आफ्नो सिर्जना बिना अनुमति प्रयोग हुने समस्या जस्ता मुद्दाहरू सामना गर्दैछन्। यस्ता चुनौतीहरूलाई समाधान गर्न कानूनी संरचना, पारिश्रमिकका मापदण्ड, र डिजिटल प्लेटफर्महरूको जिम्मेवारी सुनिश्चित गर्नु आवश्यक छ।

सिफारिसहरू:

- → नेपालमा डाटा सुरक्षा ऐन बनाउन आवश्यक छ र गोपनीयता सम्बन्धी कानुनी संरचनालाई सुदृढ गर्नु पर्छ।
- → साइबर सुरक्षा प्रणालीलाई बलियो बनाउने उद्देश्यले उच्चस्तरीय सुरक्षा पूर्वाधारको विकास गर्नुपर्छ।
- → सरकारी वेबसाइट र डिजिटल सेवा प्रदायकहरूको साइबर आक्रमणबाट सुरक्षा गर्न विशेष सुरक्षा उपायहरू अपनाउनु पर्छ।
- → क्रसबोर्डर भुक्तानी सेवामा व्यक्तिगत डाटाको सुरक्षा सुनिश्चित गर्न कानुनी प्रावधानहरू कडा गर्नु पर्छ।
- → सीमान्तकृत समुदायका लागि डिजिटल सेवामा सहज पहुँच सुनिश्चित गर्न समावेशी र प्रयोगकर्ता-मैत्री डिजाइन लागू गर्नुपर्छ।
- → राष्ट्रिय परिचयपत्रमा समावेशी पहिचान प्रक्रियालाई अपनाउनु पर्छ।
- → डिजिटल हिंसा नियन्त्रणका लागि स्पष्ट कानुनी व्यवस्थापन र प्रभावकारी कार्यान्वयन सुनिश्चित गर्न आवश्यक छ।
- → अनलाइन हिंसा र सुरक्षा सम्बन्धी जनचेतना फैलाउन र डिजिटल साक्षरताका कार्यक्रमहरू सञ्चालन गर्नुपर्छ।
- → डिजिटल प्लेटफर्महरूको नियमन गर्दा प्रत्यक्ष प्रभावित समुदायसँग परामर्श गर्नुपर्छ।
- → डिजिटल श्रमिकहरूको शोषण रोक्न न्यूनतम पारिश्रमिक र पारदर्शी आम्दानी प्रणालीको सुनिश्चितता गर्नुपर्छ।
- → डिजिटल स्पेसमा स्वतन्त्र अभिव्यक्ति सुरक्षित राख्दै सेन्सरसिपबाट जोगाउनुपर्छ।
- → अदालती कारबाही र सरकारी हस्तक्षेपलाई कानुनी रूपमा स्पष्ट गर्नु पर्छ।
- → डिजिटल निगरानीको नाममा नागरिक स्वतन्त्रता कुण्ठित हुन नदिन ग्यारेन्टी गर्नु पर्छ।
- → सेन्सरसिपको दुरुपयोगको रोकथाम गर्न नागरिक समाज, मिडिया र डिजिटल प्रयोगकर्ताहरूलाई सचेत रहन प्रोत्साहित गर्नुपर्छ।

निष्कर्ष:

अन्त्यमा, यस मिडिया अनुगमन प्रतिवेदनले डिजिटल अधिकारहरूको वर्तमान स्थिति र चुनौतीहरूलाई स्पष्ट रूपमा प्रस्तुत गरेको छ। यो रिपोर्ट डिजिटल अधिकारहरूको संरक्षणमा आउने विविध अवरोध र तिनका समाधानहरूका लागि मार्गदर्शन प्रदान गर्नका लागि तयार गरिएको हो। हाम्रो उद्देश्य भनेको डिजिटल क्षेत्रमा समानता, गोपनीयता र सुरक्षा सुनिश्चित गर्दै, सबैको पहुँच र अधिकारको सम्मान गर्नु हो। यस रिपोर्टले हामीलाई डिजिटल अधिकारको प्रभावकारी प्रवर्धन र सुरक्षाका लागि आवश्यक कदमहरू चिन्न र त्यसमा आधारित रणनीतिहरू विकास गर्न मद्दत पुर्‍याउनेछ।

नोट: यस अनुगमन प्रतिवेदन हाम्रो एक्लै संस्थागत पहलबाट भएको हो। यद्यपी भुलचुकको सम्भावनालाई स्वीकार गर्दै केहि सुझाव वा प्रतिक्रिया भए communication@bodyanddata.org मार्फत इमेलमा सम्पर्कका लागी आग्रह गर्दछौँ।

अनुसूची — अनुगमन गरिएको मिडियाहरु

टेकपाना	रातोपाटी	देश सञ्चार	कान्तिपुर
गोरखापत्र	आइसिटी समाचार	खरीबोट	न्युज् २४
नेपाल लाईव	राजधानी	नागरिक दैनिक	हिमालखबर
ईमेजखबर	अन्लाईन खबर	बि.बि.सि. न्युज् नेपाल	सेतोपटी
मकालुखबर	काठमाडौँ प्रेस	शिलापत्र	उज्यालोअन्लाईन
नयाँपत्रिका	थाहाखबर	१२खरी	द राईजिंग नेपाल
माई रिपब्लिका	द हिमालयन टाइम्स	खबरहब	नेपालखबर पत्रिका
द काठमाडौँ पोस्ट	द फारसाइट नेपाल		