Digital Rights Nepal

सूचना प्रविधि र साइबर सुरक्षा विधेयक, २०८१ संक्षिप्त विश्लेषण पत्र

परिचय

नेपाल सरकारले जारी गरेको सूचना प्रविधि र साइबर सुरक्षा विधेयक, २०८१ मा साइबर सुरक्षा नीति, विद्युतीय अभिलेख र डिजिटल हस्ताक्षर, विद्युतीय माध्यमबाट सार्वजनिक सेवा प्रवाह, संवेदनशील सूचना संरचनाको सुरक्षा, साइबर सुरक्षा सेवा प्रदायकहरूलाई अनुमति र उनीहरूको नियमन लगायतका विषयहरू समावेश छन् । यो विधेयक नेपालको सूचना प्रविधिको विकास र साइवर सुरक्षामा महत्वपूर्ण कोशेढुंगा हुने अपेक्षा गरिएको छ । तथापि यस विधेयकलाई अधिकारमुखी, प्रभावकारी र अन्तर्राष्ट्रिय मान्यता अनुरूपको बनाउन यसमा सुधार आवश्यक छ । विधेयकमा प्रस्तावित प्रावधानहरुले अनलाईन अभिव्यक्ति स्वतन्त्रता, गोपनीयताको अधिकार, तथ्यांक संरक्षणको अधिकार, सूचनाको अधिकार आदिमा प्रभाव पार्ने सन्दर्भमा डिजिटल राइट्स नेपालले तयार गरेको यस वकालत पत्रले प्रस्तावित प्रावधानहरूले उक्त अधिकारमा कस्तो प्रभाव पार्छ र उक्त प्रावधानहरूमा कसरी सुधार गरिनुपर्छ भन्ने सुझावहरू समेत उल्लेख गरेको छ ।

१. अभिव्यक्ति स्वतन्त्रता अधिकारमा पार्ने प्रभाव

विधेयकले विभिन्न प्रकारका अस्पष्ट, फराकिला, र अपरिभाषित अनलाइन व्यवहार वा अभिव्यक्तिका प्रकारहरुमा बन्देज लगाएको छ । विधेयकमा समावेश निम्नलिखित निषेधात्मक व्यवस्थाहरूले अभिव्यक्ति स्वतन्त्रतालाई उल्लङ्घन गर्न सक्नुका साथै ICCPR को धारा १९ को तीन-भाग परीक्षणमा अनुत्तीर्ण समेत हुन्छनः

क. दफा ७९(१): "कसैले पनि विद्युतीय प्रणालीको प्रयोग गरी नेपालको राष्ट्रिय सुरक्षा, सार्वभौमसत्ता, भौगोलिक अखण्डता, राष्ट्रियता वा राष्ट्रिय एकता, स्वतन्त्रता, स्वाभिमान वा संघीय इकाईहरू बीचको सुसम्बन्ध तथा समन्वयमा बाधा पार्ने वा देशको सुरक्षा वा सूचना प्रणालीलाई असर पार्ने कुनै कार्य गर्न वा गराउन हुदैन ।"

विश्लेषण:

- यो प्रावधान धेरै व्यापक र अस्पष्ट छ, जसले असहमतिपूर्ण अभिव्यक्तिहरूलाई पनि अपराधीकरण गर्न सक्ने सम्भावना देखिन्छ ।

ख. दफा १२६(२): "कसैले पनि शान्ति सुरक्षा भङ्ग हुने कार्यलाई बढावा दिनका लागि प्रचलित कानून बमोजिम प्रकाशन वा प्रशारण गर्न रोक लगाएको कुनै कुरा प्रसारण वा संप्रेषण गर्न वा सार्वजनिक सदाचार र नैतिकताको प्रतिकूल हुने कुनै कार्य गर्नका लागि विद्युतीय सञ्चार माध्यमको प्रयोग गर्नु हुदैन ।"

विश्लेषण:

- यो प्रावधानले असहमति वा आलोचनात्मक विचार व्यक्त गर्नमा रोक लगाउन सक्छ ।

ग. दफा ११५: "कसैले पनि विद्युतीय प्रणाली प्रयोग गरेर अरूलाई हैरान, गिज्याउने, जिस्काउने, निराश गराउने, अपमान गर्ने वा दुर्व्यवहार गर्न हुदैन ।"

विश्लेषण:

- दफा ११५ को व्यवस्था ज्यादै व्यापक र अस्पष्ट छ जसका कारण व्यक्तिहरू कुन सामग्री "अपमानजनक" ठहरिने हो भनेर पूर्वानुमान गर्न सक्दैनन् । प्रावधानमा निहित व्यापकता र अस्पष्टताका कारण ICCPR को धारा १९ बमोजिमको "कानूनद्वारा व्यवस्था गरिएको" परीक्षण पूरा हुन सक्दैन ।

सुझाव

- दफा ७९(१) र १२६(२) बमोजिमका निषेधित अनलाइन कार्यलाई विधेयकबाट हटाइनुपर्छ । अन्य व्यक्तिको अधिकार वा प्रतिष्ठा, राष्ट्रिय सुरक्षा वा सावर्जनिक व्यवस्था, वा सार्वजनिक स्वास्थ्य वा नैतिकताको रक्षाका लागि केही निश्चित प्रकारको अनलाइन व्यवहार वा अभिव्यक्तिलाई प्रतिबन्धित गर्न आवश्यक भएमा, त्यस्ता बन्देज लगाइनुपर्ने अनलाइन अभिव्यक्ति र व्यवहारका प्रकारहरूलाई "कानूनद्वारा प्रदान गरिएको" परीक्षण अनुरूप बनाउन स्पष्ट रूपमा परिभाषा गरिनुपर्छ ।

- अभिव्यक्तिको स्वतन्त्रताको अधिकारलाई सुनिश्चित गर्न धारा ११५ मा सुधार गरिनु पर्दछ ।

२. गोपनियताको अधिकारमा पार्ने प्रभाव

क. दफा १४४: यस दफामा यदि कुनै अनुसन्धान अधिकारीले "खानतलास गर्ने क्रममा, कुनै व्यक्ति, जो सम्बन्धित मुद्दामा आरोपी होइन, उसको नियन्त्रणमा कुनै विद्युतीय उपकरण वा जानकारी फेला पारेमा सो व्यक्तिले अधिकारीलाई उक्त उपकरण वा विद्युतीय डाटा पहुँच गर्न, त्यसको प्रतिलिपि डाउनलोड गर्न, एन्क्रिप्ट गरिएको जानकारी डिक्रिप्ट गर्न, र अन्य आवश्यक सहायता प्रदान गर्न अनुमति दिनुपर्छ" भन्ने व्यवस्था रहेको छ।

प्रमुख चासो

यस प्रावधानले ICCPR द्वारा संरक्षित गोपनीयताको अधिकारमा अत्यधिक र स्वेच्छाचारी हस्तक्षेप गर्ने भएकाले समस्याजनक छ। यसले कुनै पनि व्यक्तिलाई कुनै अपराधमा संलग्न रहेको आशङ्का नगरिएको वा आरोप नलागेको अवस्थामा समेत अनुसन्धान अधिकारीसमक्ष आफ्नो विद्युतीय उपकरण र डाटा पहुँच गर्न र डिक्रिप्ट गर्न बाध्य बनाउँछ। यसले सरकारलाई व्यक्तिहरूको विद्युतीय उपकरण र डाटामा पहुँच प्राप्त गर्न र त्यसको नियन्त्रण गर्न निर्बाध तवरमा अनुमति दिन्छ।

सुझाव

विधेयकबाट दफा १४४ लाई हटाइनुपर्छ। यदि यो प्रावधान पूर्ण रूपमा नहटाउने हो भने विधेयकका मस्यौदाकारहरूले अनुसन्धान अधिकारीलाई व्यक्तिको विद्युतीय उपकरण वा डाटा पहुँच गर्न वा यस प्रावधानमा वर्णित तरिकामा डाटा डिक्रिप्ट गर्न अदालतबाट आदेश (वारंट) प्राप्त गर्नुपर्ने भन्ने वाक्यांश समावेश गरिनु पर्दछ।

३. सामाग्री हटाउने (टेक डाउन) आदेश र मध्यस्थकर्ताको जिम्मेवारी

क. दफा ९२: विधेयकको यस दफाको प्रतिबन्धात्मक वाक्यांशले तेस्रो पक्षद्वारा पहुँच गरिएका अवैध सामग्रीको लागि सेवा प्रदायकहरूलाई आपराधिक रूपले जिम्मेवार ठहराउने व्यवस्था गरेको छ। यसले सेवाप्रदायकहरूलाई अनावश्यक जोखिममा पार्छ र स्वतन्त्र इन्टरनेटको अवधारणालाई चुनौती दिन सक्छ।

प्रमुख चासो

- नोटिस-एन्ड-टेकडाउन प्रणालीमा सेवा प्रदायकले टेकडाउन आदेशको पालना गरेमा सामान्यतः उसले जिम्मेवारी बहन गर्नु पर्दैन। तथापि, दफा ९२ को दुरूपयोगको हुनसक्छ र त्यसबाट अभिव्यक्ति स्वतन्त्रतामा बन्देजको सम्भावना रहन्छ।

- यस अन्तर्गत पहिलो चिन्ताजनक विषय भनेको कुनै पनि "सम्बन्धित सार्वजनिक निकाय" ले अवैध अभिव्यक्ति भनी आरोपित सामग्रीका सम्बन्धमा कुनै विशिष्ट चासो वा सम्बन्ध नभएको अवस्थामा पनि उक्त सामग्री हटाउने आदेश जारी गर्न सक्ने व्यवस्थाले अनलाइन सामग्री हटाउनका लागि धेरै अनावश्यक अनुरोधहरू आउन सक्ने सम्भावना रहन्छ। त्यस्तै, दुर्व्यवहार गर्न वा राजनीतिक कारणले वा बदला लिनका लागि पनि सामग्री हटाउने आदेश प्रणालीको दुरुपयोग हुन सक्ने सम्भावना समेत रहन्छ।

- दोस्रो, जसको सामग्रीलाई आपत्तिजनक वा प्रतिबन्धित ठहर गरिएको हो तिनीहरूले सो सामग्री हटाउने आदेश उपर चित्त नबुझेमा चुनौती दिने अवसर समेतको व्यवस्था छैन। दफा ९२ ले आपत्तिजनक वा प्रतिबन्धित सामग्री "यथासिघ्र" हटाउने वा पहुँच निष्कृय गर्नुपर्ने व्यवस्था गरेको छ, अन्यथा सेवा प्रदायकले आपराधिक जिम्मेवारी वहन गर्नुपर्छ। सामग्री हटाउने आदेश विरुद्ध चुनौती दिने कुनै उपायको अभावमा अधिक सेन्सरसीप हुने सम्भावना छ, र यसबाट अभिव्यक्तिको स्वतन्त्रताको एक अभिन्न पाटोको रूपमा रहेको सूचनाको स्वतन्त्र प्रवाहमा बन्देज लाग्दछ।

- तेस्रो, दफा ९२ मा सामग्री हटाउने आदेशको पालना नगर्ने संस्थाहरूले मध्यस्थ जिम्मेवारी वहन प्रावधानको व्यवस्था छ। सामग्री हटाउनुपर्ने सूचना आए पछि नहटाएमा फौजदारी दायित्व बहन गर्नुपर्ने र सामग्री प्रकाशकलाई उपचारको कुनै व्यवस्था नभएकाले सामाजिक सञ्जाल प्लेटफर्महरूले सामग्री हटाउने सूचना प्राप्त गरेपछि जुनै पनि सामग्रीलाई हटाउने हुन्छन्।

- अन्ततः दफा ९२ ले यदि "कुनै सूचना, तथ्याङ्क वा लिंकमा उल्लेख वा समावेश भएको कुनै तथ्य वा विवरणले प्रचलित कानूनको उल्लघंन गरेमा वा कुनै गैरकानूनी कार्य गर्न दुरुत्साहन वा सहयोग गरेमा सेवा प्रदायकले दायित्व वहन गर्नुपर्ने" व्यवस्था गरेको छ। अर्को शब्दमा, यदि तेस्रो पक्ष सामग्री अवैध छ भने सेवा प्रदायक जिम्मेवार हुनेछ। यो व्यवस्था मध्यस्थ जिम्मेवारीको अपवादको उद्देश्य विपरीत छ, किनकी अपवादको उद्देश्य नै सेवा प्रदायकको प्लेटफर्ममा प्रकाशित तेस्रो पक्ष सामग्री अवैध रैछन् भने सेवा प्रदायकहरूलाई सो को जिम्मेवारीबाट मुक्त गर्नु हो।

सुझाव

सामग्री हटाउनका लागि अदालतको आदेश अनिवार्य रूपमा आवश्यक पर्ने व्यवस्था गरिनुपर्छ। यस प्रावधानमा आपत्तिजनक वा प्रतिबन्धित भनिएका सामग्रीका प्रकाशकहरूले त्यस्ता सामग्री हटाउने आदेशका विरुद्द स्वतन्त्र, निष्पक्ष न्यायालय वा न्यायिक निकाय समक्ष चुनौती दिन पाउने अनिवार्य कानूनी व्यवस्था समेट्ने भाषा समावेश गरिनुपर्छ।

४. डाटा संरक्षणसम्बन्धी अधिकारमा पार्ने प्रभाव

क. दफा ३८(१): विधेयकका प्रावधानहरूको उल्लङ्घनको शङ्का लागेको खण्डमा दफा ३८(१) ले नियन्त्रकलाई "कुनै पनि कम्प्युटर प्रणाली, उपकरण, यन्त्र, डाटा, सूचना प्रणाली वा यस्तो प्रणालीसँग सम्बन्धित कुनै पनि सामग्री" पहुँच प्राप्त गर्ने व्यापक अधिकार प्रदान गर्छ। न्यायिक अनुमतीको प्राप्त गर्नुपर्ने नभएकाले यस प्रावधानले गोपनीयताको अधिकारमा जोखिम उत्पन्न गर्छ।

विश्लेषण:

- यस दफामा प्रयोग भएको भाषा अत्यन्त व्यापक छ र नियन्त्रकबाट यस अधिकारको दुरुपयोग नहोस् भनी सुनिश्चित गर्न न्यायिक निरीक्षणको व्यवस्था तथा व्यक्तिको कम्प्युटर प्रणाली वा डाटा पहुँच गर्न अनुमती प्राप्त गर्नुपर्ने व्यवस्था जस्ता सुरक्षा उपायहरू समावेश छैन। न्यायिक निरीक्षण बिना व्यक्तिहरूको कम्प्युटर प्रणाली र व्यक्तिगत डाटा पहुँच गर्न व्यापक रुपमा कानून कार्यन्वयनकर्तालाई अनुमति दिनाले अभिव्यक्ति स्वतन्त्रता र गोपनीयताको अधिकारमा अनुपयुक्त बन्देजको सम्भावना रहन्छ।

ख. दफा ८०: दफा ८० ले "व्यक्तिगत जानकारी" सङ्कलनसँग सम्बन्धित विभिन्न नियमहरूको व्यवस्था गर्दछ, जसअन्तर्गत कसैले पनि प्रचलित कानून बमोजिम बाहेक कसैको व्यक्तिगत जानकारी सङ्कलन गर्न नहुने, यदि कसैको व्यक्तिगत जानकारी सङ्कलन गर्नुपर्छ भने, सम्बन्धित व्यक्तिलाई सो विवरणहरू किन आवश्यक छन् भन्ने बारे जानकारी दिनुपर्ने, सूचना प्रविधि प्रणालीमा भण्डारण गरिएका कुनै पनि व्यक्तिको व्यक्तिगत विवरणहरू सङ्कलन गर्दा उल्लेख गरिएको उद्देश्यबाहेक अन्य उद्देश्यको लागि प्रयोग गर्न, प्रचार गर्न, वा साझा गर्न नहुने, र सङ्कलन तथा भण्डारणको उद्देश्य समाप्त भएपछि, सङ्कलन र भण्डारण गरिएको कुनै पनि व्यक्तिगत जानकारी ३५ दिनभित्र नष्ट गर्नुपर्छ।

विश्लेषण:

- दफा ८० ले "व्यक्तिगत विवरण" सङ्कलन गर्ने निकायले सम्बन्धित व्यक्तिलाई सूचित गर्नुपर्ने, उक्त जानकारीको प्रयोग सीमित रूपमा गर्नुपर्ने, र सङ्कलन तथा भण्डारणको उद्देश्य समाप्त भएको पैतिस दिनभित्र जानकारी नष्ट गर्नुपर्ने व्यवस्था गरेर "व्यक्तिगत जानकारी" सङ्कलनसँग सम्बन्धित गोपनीयता संरक्षणलाई सुदृढ पार्ने उद्देश्य राखेको देखिन्छ।

यी व्यवस्थाहरू GDPR जस्ता तथ्यांक संरक्षण ढाचाका आधारभूत सिद्धान्त अनुरुप भए पनि यी प्रावधानहरू विस्तृत तथ्यांक संरक्षण कानूनको प्रभावकारी विकल्प भने बन्न सक्दैनन्।सरकारले यो प्रावधानहरू हटाएर यसको सट्टा GDPR जस्ता अन्तर्राष्ट्रिय ढाचामा आधारित छुट्टै तथ्यांक संरक्षण कानून तयार गर्ने बारेमा विचार गर्नुपर्छ।

सुझाव

दफा ३८(१) लाई संशोधन गरी गोपनीयताको सुरक्षा गर्न वारंट वा न्यायालय वा अन्य सक्षम, स्वतन्त्र निकायबाट आदेश प्राप्त गर्न आवश्यक पर्ने जस्ता गोपनीयताको सुरक्षा उपायहरू समावेश गर्नुपर्छ। त्यसैगरी, डाटा तथा प्रणालीमा पहुँचको अधिकारलाई दुरुपयोग हुन नदिनका लागि स्पष्ट मापदण्डहरू निर्धारण गर्नुपर्छ, र कार्यान्वयनमा पारदर्शिता तथा उत्तरदायित्व सुनिश्चित गर्न स्वतन्त्र निकायद्वारा अनुगमनको व्यवस्था गर्नुपर्छ। यसले नागरिक अधिकारको रक्षा गर्दै कानूनी प्रक्रिया पारदर्शी र जवाफदेही बनाउनेछ।

दफा ८० हटाउनुपर्छ र नागरिक समाज लगायतका सरोकारवालाहरूसँग विशेषिकृत तथ्यांक संरक्षण कानूनले तथ्यांक सुरक्षा र गोपनीयताको अधिकारलाई प्रवर्धन गर्छ वा गर्दैन भन्ने सम्बन्धमा परामर्श गरिनु पर्दछ।

५. संवेदनशील सूचना पूर्वाधार सम्बन्धी व्यवस्था

विधेयकमा "संवेदनशील सूचना पूर्वाधार" को धनिले राष्ट्रिय साइबर सुरक्षा केन्द्रलाई आवश्यक परेको सुचना माग भएको अवस्थामा उपलब्ध गराउने, वार्षिक सुरक्षा अडिट सञ्चालन गर्ने र सो को नतिजा केन्द्रमा पेश गर्ने, समय-समयमा साइबर सुरक्षा अभ्यास गर्ने, र संवेदनशील सूचना संरचनासँग सम्बन्धित साइबर सुरक्षा घटनाहरूका बारेमा जानकारी गराउनु पर्ने व्यवस्था छ (दफा १०५ - १०९)। साथै, विधेयकले राष्ट्रिय साइबर सुरक्षा केन्द्रलाई "संवेदनशील सूचना पूर्वाधार" को "चौबिसै घण्टा अनुगमन" गर्न निर्देशन गरेको छ (दफा ९४)। तर, विधेयकले "संवेदनशील सूचना पूर्वाधार" को परिभाषा भने गरेको छैन।

यसको साटो दफा १०४ ले सरकारलाई नेपाल राजपत्रमा सूचना प्रकाशित गरेर "संवेदनशील सूचना पूर्वाधार" तोक्न सक्ने अधिकार दिएको छ। यस्तो प्रावधानलाई सरकारले निश्चित व्यक्ति वा समूहहरू र त्यसमा पनि विशेषगरी सरकारी नीतिको आलोचकहरूको सूचना संरचनामा स्वेच्छाचारी बन्देज लगाउन दुरूपयोग गर्नसक्ने जोखिम रहन्छ।

अन्य देशहरूका उदाहरण

- युरोपेली संघमा 'महत्त्वपूर्ण सूचना संरचना' (Critical Informatin Infrastructure) अन्तर्गत ऊर्जा, बैंकिङ, यातायात लगायतका विशिष्ट क्षेत्रहरू पहिचान गरिएका छन्। विधेयकमा पनि यस किसिमको स्पष्टता आवश्यक छ।

सुझावहरू:

'संवेदनशील सूचना संरचना'को स्पष्ट र पारदर्शी परिभाषा विधेयकमा समावेश गर्नुपर्छ।
सरकारले "संवेदनशील सूचना संरचना" क्षेत्रहरू पहिचानका लागि जोखिम मूल्याङ्कन गरी सोको निष्कर्ष प्रकाशन गर्नुपर्छ।
कानूनको दायरा अस्पष्ट र व्यापक नहुने सुनिश्चित गर्न उक्त मूल्याङ्कन प्रतिबिम्बित हुने गरी दफा १०४ अद्यावधिक गर्नुपर्छ।

निष्कर्ष

सूचना प्रविधि तथा साइबर सुरक्षा विधेयक, २०८१ ले नेपालमा साइबर सुरक्षालाई सुदृढ र सूचना प्रविधिको नियमनलाई बलियो बनाउनेछ। तर साथसाथै यस विधेयकमा रहेका केहि प्रावधानहरू, उदाहरणका लागि अनलाइन व्यवहार र अभिव्यक्तिमा अस्पष्ट निषेधहरू, मध्यस्थ जिम्मेवारीको दायित्व, अनुसन्धानको क्रममा अधिकारीहरुलाई व्यक्तिहरूले आफ्ना विद्युतीय उपकरणहरूमा पहुँचको अनुमति दिनुपर्ने व्यवस्था लगायत यस विश्लेषण पत्रमा उल्लिखित प्रावधानहरूले अनलाइन अभिव्यक्तिको स्वतन्त्रता र गोपनियताको हकलाई कमजोर बनाउन सक्छ। अभिव्यक्ती स्वतन्त्रता तथा गोपनियताको हक सुनिश्चित गर्दै साइबर सुरक्षा प्रवर्धन र प्रत्याभुत गर्न मस्यौदाकारहरूले यस विधेयकका प्रावधान उपरका उल्लिखित चासोहरूलाई सम्बोधन गर्नुपर्छ।

हाम्रो बारेमा

प्रविधि अधिकार नेपाल (DRN) सन् २०२० मा स्थापित नेपालमा डिजिटल अधिकारको संरक्षण र सुरक्षित अनलाइन वातावरणको विकासमा समर्पित गैर नाफामूलक संस्था हो । नागरिक अधिकार अभियन्ताहरु तथा विशेषज्ञहरु संलग्न प्रविधि अधिकार नेपालले अनलाइन अभिव्यक्ति स्वतन्त्रता, गोपनीयता संरक्षण, सूचनामा पहुँच, र साइबर सुरक्षा प्रवर्धन गर्न क्षमता अभिवृद्धि पहलहरूमा संलग्न रहदै अनुसन्धान, अध्ययन तथा नीति सुधारका लागि वकालत गर्दछ । मानव अधिकार र डिजिटल अधिकार वकालतकर्ताहरुका नेतृत्वमा प्रविधि अधिकार नेपालले स्थानीय तथा अन्तर्राष्ट्रिय स्तरमा नेपालको डिजिटल परिदृश्यलाई सशक्त बनाउन महत्वपूर्ण भूमिका निभाएको छ। प्रविधि अधिकार नेपालको कामको बारेमा थप जानकारीको लागि, कृपया www.igitalrightsnepal.org मा जानुहोस् ।

Digital Rights Nepal

Phone: +977-9767245100
Address: Neel Saraswoti Marga, Gairidhara - 2, Kathmandu
Email: info@digitalrightsnepal.org
Web: www.digitalrightsnepal.org