सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धमा व्यवस्था गर्न बनेको विधेयक

विश्लेषण पत्र

२०८२

Digital Rights Nepal

परिचय

सूचना प्रविधिको विकास, प्रवर्द्धन तथा नियमन गर्न, विद्युतीय अभिलेख तथा डिजिटल हस्ताक्षरको सत्यता र विश्वसनीयता कायम राख्न, साइबर स्पेसमा रहेका सूचना, तथ्याङ्क वा विवरणको संरक्षण तथा व्यवस्थित प्रयोग गर्न र साइबर सुरक्षा सम्बन्धी प्रचलित कानुनलाई संशोधन र एकीकरण गर्ने उद्देश्यका साथ सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धमा व्यवस्था गर्न बनेको विधेयक २०८२ जेष्ठ २७ मा प्रतिनिधि सभामा दर्ता भएको थियो। २०८२ साउन २९ गते सञ्चार तथा सूचना प्रविधि मन्त्रीद्वारा प्रस्तुत यस विधेयकमा छलफल पश्चात् ७२ घण्टे संशोधन प्रस्ताव खुल्ला गरिएको छ ।

विधेयकले समेटेका मुख्य क्षेत्रहरू

यस विधेयकमा विद्युतीय स्वरूपका अभिलेखलाई कानुनी मान्यता, डिजिटल हस्ताक्षर, डोमेन नाम दर्ता तथा व्यवस्थापन, सूचना प्रविधि व्यवसाय, डाटा सेन्टर तथा क्लाउड सेवा, सेवा प्रदायकको दायित्व, साइबर सुरक्षा केन्द्रको स्थापना तथा कार्यादेश, संवेदनशील सूचना पूर्वाधार लगायतका विषयहरू समेटिएका छन् भने साइबर अपराध तथा कसुर र सजायका व्यवस्था समेत गरिएको छ ।

विधेयकमा रहेका केही समस्याजनक प्रावधान

१. अभिव्यक्ति स्वतन्त्रतामा असर

विधेयकको दफा ८८ (१) मा कुनै पनि विद्युतीय प्रणाली वा माध्यमबाट अश्लील सामग्रीको उत्पादन, सङ्कलन, बिक्री, वितरण, प्रकाशन, प्रसारण, प्रदर्शन गर्न वा गराउन नहुने उल्लेख गरिएको छ। साथै यस कार्यमा संलग्न हुने व्यक्तिका लागि दुई वर्ष सम्म कैद वा दुई लाख जरिबाना वा दुवै सजाय हुने व्यवस्था समेत गरिएको छ। तथापि यस दफामा 'अश्लील सामग्री' भन्नाले के बुझिन्छ भन्ने स्पष्ट परिभाषा दिइएको छैन ।

यस खालको अस्पष्टता कानुनी दृष्टिले निकै जटिल र समस्याजनक हुन सक्छ। "अश्लीलता" एक सापेक्षिक अवधारणा हो, जसको व्याख्या सामाजिक, सांस्कृतिक र कानुनी सन्दर्भ अनुसार फरक-फरक हुन्छ। तर, विधेयकले त्यसको कुनै कानुनी परिभाषा वा मापदण्ड नतोकी, सिधै निषेधात्मक भाषा प्रयोग गरी यो कार्यलाई अपराधको रूपमा व्याख्या गरेको छ । मिडियामा प्रकाशन भएका, आम नागरिकले अभिव्यक्त गरेका वा कुनै कलाकारले आफ्नो कल्पनाशीलता प्रकट गर्दै बनाएका सिर्जनाहरू कुनै नियामक निकायलाई "अश्लील" लागेको खण्डमा यस दफाको दुरुपयोग हुन सक्छ र अभिव्यक्ति स्वतन्त्रता, कलात्मक स्वतन्त्रता र डिजिटल माध्यममा स्वतन्त्र विचार प्रस्तुत गर्ने अधिकारमाथि प्रत्यक्ष असर पुऱ्याउन सक्छ ।

सुझाव:

विधेयकमा 'अश्लील सामग्री' ले सिर्जना गर्ने सामाजिक जोखिमका आधारमा स्पष्ट, सन्दर्भगत र मान्यता प्राप्त कानुनी परिभाषा समेट्नु आवश्यक छ ।

२. डाटा सुरक्षासम्बन्धी व्यवस्था

- क) वैयक्तिक गोपनीयता सम्बन्धी:

विधेयकको परिच्छेद १० ले वैयक्तिक विवरण तथा सूचनाको सुरक्षा सम्बन्धी व्यवस्था गरेको छ । दफा ६१ ले "वैयक्तिक विवरण" सङ्कलनसँग सम्बन्धित विभिन्न नियमहरूको व्यवस्था गर्दछ, जसमा निम्न कुरा समावेश छन:

- कसैले पनि प्रचलित कानुन बमोजिम बाहेक कसैको व्यक्तिगत जानकारी सङ्कलन गर्न हुँदैन ।
- यदि कसैको व्यक्तिगत जानकारी सङ्कलन गर्नुपर्छ भने, सम्बन्धित व्यक्तिलाई सो विवरणहरू किन आवश्यक छन् भन्ने बारे जानकारी दिनुपर्छ ।
- 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 हुँदैन ।
- सङ्कलन र भण्डारणको उद्देश्य समाप्त भएपछि, सङ्कलन र भण्डारण गरिएको कुनै पनि व्यक्तिगत जानकारीलाई ३५ दिनभित्र नष्ट गर्नुपर्छ ।

विश्लेषण: दफा ६१ ले "वैयक्तिक 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 "वैयक्तिक विवरण" सङ्कलनसँग सम्बन्धित गोपनीयता संरक्षणलाई सुदृढ पार्ने उद्देश्य राखेको देखिन्छ ।

विधेयकको यी प्रावधानहरूले वैयक्तिक विवरण र सूचना सम्बन्धी केही राम्रो व्यवस्था गरेको भएता पनि यी व्यवस्था अपुरा छन् । विधेयकमा वैयक्तिक विवरण र सूचनामा तथ्याङ्कधारक व्यक्ति (Data Subject) को के कस्तो अधिकार हुने भन्ने बारेमा कुनै व्यवस्था छैन । उदाहरणका लागि, विधेयकमा जसको तथ्यांक हो उसलाई आफ्नो तथ्याङ्कमा पहुँचको अधिकार, गलत डाटालाई सुधार गर्ने अधिकार, आफ्नो डाटा मेटाउने अधिकार, आफ्नो डाटाको अनुचित प्रयोग रोक्ने वा त्यसको विरोध गर्ने अधिकार, स्वचालित निर्णय/प्रोफाइलिङ विरुद्धको संरक्षण लगायतका विषयवस्तु समेटिएका छैनन् ।

स्वास्थ्य, वित्त, दूरसञ्चार, शिक्षा जस्ता क्षेत्रसँग जोडिएका तथ्यांक संवेदनशील तथ्याङ्क हुन्। तथापि यस्ता संवेदनशील तथ्याङ्कका सम्बन्धमा इन्कृप्सनबाहेक अन्य कुनै विशेष सुरक्षा उपायको व्यवस्था गरिएको छैन र यसबाट डाटा उल्लङ्घन वा दुरुपयोग हुादा ठुलो हानी हुन सक्छ। त्यसै गरी विधेयकमा व्यक्तिगत डेटा नेपाल बाहिर जाादा वा पठाउादा (Cross-border data transfer) कस्तो मापदण्ड पालना गर्नुपर्ने भन्ने प्रावधान छैन भने डाटा दुरुपयोगका पीडितका लागि स्पष्ट उजुरी प्रक्रियाको व्यवस्था समेत छैन।

डाटा संरक्षण सम्बन्धी केही विषय सूचना प्रविधि तथा साइबर सुरक्षाको विषय भएता पनि डाटा संरक्षणको लागि छुट्टै विशेषकृत कानुन आवश्यक हुन्छ। नेपाल सरकारले डिजिटल तथ्याङ्क संरक्षणसम्बन्धी कानुनको मस्यौदाका काम गरिरहेको सन्दर्भमा यस कानुनमा साइबर सुरक्षासाग सम्बन्धित डाटा/सूचना संरक्षणको विषयलाई डाटा संरक्षण सिद्धान्तका आधारमा समेट्दै GDPR जस्ता डाटा संरक्षण ढाँचा अनुरूपको विस्तृत डाटा संरक्षण कानुनलाई प्राथमिकता दिइनुपर्छ।

सुझाव:

विधेयकमा साइबर सुरक्षासँग सम्बन्धित डाटा/सूचना संरक्षणको विषयलाई डाटा संरक्षण सिद्धान्तका आधारमा परिमार्जन गरिनु र नसमेटिएका विषयहरूलाई समेटिनु पर्छ। साथै डाटा संरक्षणसम्बन्धी विशेषकृत कानुन निर्माणलाई प्राथमिकता दिनु आवश्यक छ।

ख. सूचना सुरक्षित राख्नु पर्ने सम्बन्धी व्यवस्था (दफा ६५)

विधेयकको दफा ६५ मा सेवा प्रदायकले सेवा सम्बन्धी तोकिए बमोजिमका सूचना तोकिएको अवधिसम्म सुरक्षित राख्नु पर्नेछ भनी व्यवस्था गरिएको छ। यो व्यवस्था अस्पष्ट र अधुरो देखिन्छ। "तोकिएको" भनी उल्लेख गरिएको भए पनि कुन कानुन वा नियामक निकायबाट सूचना राख्ने अवधि तोकिने हो भन्नेबारे स्पष्ट जानकारी छैन। यस्तो खुला र अस्पष्ट शब्दावलीले सेवा प्रदायकलाई अनिश्चितताामा पार्न सक्छ र प्रयोगकर्ताको डाटा संरक्षण सम्बन्धी अधिकारमा पनि अस्पष्टता उत्पन्न गराउँछ। विधेयकको दफा १११ र ११२ मा उल्लेखित नियम बनाउने तथा मापदण्ड बनाउने प्रावधानअन्तर्गत पनि यो विषय समेटिएको छैन।

यदि डाटा सुरक्षित राख्नुपर्ने अवधि स्पष्ट रूपमा नतोकिने हो भने, सेवा प्रदायकहरूले आवश्यकता भन्दा बढी समयसम्म प्रयोगकर्ताको व्यक्तिगत डाटा राख्न सक्नेछन्, जसले डाटा न्युनीकरण (data minimization), उद्देश्य सीमितता (purpose limitation) र डाटा मेटाउने अधिकार (right to erasure) जस्ता आधारभूत डाटा संरक्षण सिद्धान्तहरूमा प्रतिकूल असर पार्न सक्छ। साथै, यो व्यवस्था अनावश्यक निगरानी, प्रयोगकर्ताको ट्र्याकिङ, र निजता हनन जस्ता जोखिमसमेत निम्त्याउन सक्छ।

सुझाव:

यस व्यवस्थामा डाटा राख्ने न्यूनतम र अधिकतम समय सीमा, तथा तिनको कानुनी आधार सुनिश्चित गर्ने स्पष्ट उल्लेख हुनुपर्ने आवश्यक देखिन्छ। डाटा संरक्षणको दृष्टिले "तोकिएको अवधिसम्म" भन्नु कानुनी रूपमा अपूरो, व्याख्यायोग्य र सम्भावित रूपमा दुरुपयोग हुने गरी खुला प्रावधान हो।

ग. सुरक्षा मापदण्ड अवलम्बन गर्नुपर्ने सम्बन्धी व्यवस्था: (दफा ६३)

सरकारी निकाय तथा सार्वजनिक संस्थाले कम्प्युटर तथा सूचना प्रणालीको प्रयोग गर्दा सुरक्षा मापदण्ड अवलम्बन गर्नु पर्नेछ भनी व्यवस्था गरेको छ। तर विधेयकले त्यस्ता सुरक्षा मापदण्ड के हुन् भन्ने कुनै स्पष्ट विवरण दिएको छैन। बरु दफा ११२ मा साइबर सुरक्षाको मापदण्डसँगै अन्य विभिन्न विषयसाग सम्बन्धित मापदण्ड मन्त्रालयले बनाउने भन्ने खुला व्यवस्था मात्र गरिएको छ।

सुझाव:

विधेयकमा कम्तीमा पनि सुरक्षा मापदण्ड निर्माणका सिद्धान्त, पारदर्शी प्रक्रिया, तथा अनिवार्य सरोकारवाला परामर्शको व्यवस्था हुनु अत्यावश्यक देखिन्छ।

विधेयकमा दफा ६३ र दफा ११२ अन्तर्गत उल्लेख भएको "सुरक्षा मापदण्ड" सम्बन्धी प्रावधानलाई अझ प्रभावकारी र जिम्मेवार बनाउन निम्न व्यवस्था समावेश हुनुपर्छ।

- सैद्धान्तिक स्पष्टता: मापदण्ड निर्माणका लागि न्यूनतम सिद्धान्तहरू (पारदर्शिता, सरोकारवाला परामर्श, मानव अधिकारको सम्मान, अन्तर्राष्ट्रिय मान्यता) विधेयकमै स्पष्ट पार्नुपर्छ।
- अनिवार्य परामर्श: मापदण्ड निर्माणका क्रममा सरकारी निकाय, प्राविधिक विज्ञ, निजी क्षेत्र, नागरिक समाज, र मानव अधिकार संस्थासँग परामर्श गरिनुपर्ने व्यवस्था गर्नुपर्छ।
- पारदर्शी प्रक्रिया: मापदण्डको प्रारूप सार्वजनिक गर्ने र लिखित राय माग गर्ने कानुनी प्रावधान राखिनुपर्छ।
- नियमित समीक्षा: प्रविधि र साइबर जोखिम दुवै परिवर्तनशील हुने भएकाले निश्चित अवधिमा मापदण्डको समीक्षा र अद्यावधिक गरिने कानुनी व्यवस्था गरिनुपर्छ।

३. संवेदनशील सूचना पूर्वाधार सम्बन्धि व्यवस्था

विधेयकले "संवेदनशील सूचना पूर्वाधार" को धनीले राष्ट्रिय साइबर सुरक्षा केन्द्रलाई आवश्यक परेको सूचना माग भएको अवस्थामा उपलब्ध गराउने, वार्षिक सुरक्षा अडिट सञ्चालन गर्ने र सो को नतिजा केन्द्रमा पेस गर्ने, समय-समयमा साइबर सुरक्षा अभ्यास गर्ने, र संवेदनशील सूचना संरचनासँग सम्बन्धित साइबर सुरक्षा घटनाहरूका बारेमा जानकारी गराउनु पर्ने व्यवस्था गरेको छ (दफा ५५ - ५८)।

साथै, विधेयकले राष्ट्रिय साइबर सुरक्षा केन्द्रलाई "संवेदनशील सूचना पूर्वाधार" को "चौबिसै घण्टा अनुगमन" गर्न निर्देशन गरेको छ (दफा ४७)। तर, विधेयकले "संवेदनशील सूचना पूर्वाधार" को परिभाषा भने गरेको छैन। राष्ट्रिय साइबर सुरक्षा केन्द्रको प्रकृति अनुसार यसको कार्यादेश "संवेदनशील सूचना पूर्वाधार" को साइबर सुरक्षा सुदृढीकरणमा नीतिगत तथा प्राविधिक रूपमा सहयोग पुऱ्याउनु हो, त्यसको अनुगमन गर्नु होइन। "संवेदनशील सूचना पूर्वाधार धनी" को परिभाषामा व्यक्तिलाई पनि समेटिएकोले यसमा व्यक्तिगत, व्यावसायिक सूचना पूर्वाधार पनि समावेश हुने देखिन्छ। "संवेदनशील सूचना पूर्वाधार' चौबिसै घण्टा अनुगमन" ले नियामक निकायको निरन्तर निगरानी सिर्जना गर्दछ भने यसले निजी व्यवसायीको व्यावसायिक गोप्यतामा समेत असर गर्दछ। 'संवेदनशील सूचना पूर्वाधारको चौबिसै घण्टा अनुगमन' सैद्धान्तिक रूपमा नै राष्ट्रिय साइबर सुरक्षा केन्द्रको क्षेत्राधिकारअन्तर्गत पर्दैन। तसर्थ "संवेदनशील सूचना पूर्वाधारको चौबिसै घण्टा अनुगमन गर्ने तथा" हटाउनुपर्ने देखिन्छ।

यसको साटो दफा ५४ 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 विशेष गरी सरकारी नीतिको आलोचकहरूको सूचना संरचनामा स्वेच्छाचारी बन्देज लगाउन दुरुपयोग गर्न सक्ने जोखिम रहन्छ।

संवेदनशील सूचना पूर्वाधार सम्बन्धमा अन्य देशहरूको अभ्यास हेर्ने हो भने युरोपेली सङ्घमा 'महत्त्वपूर्ण सूचना संरचना' (CII) अन्तर्गत ऊर्जा, बैङ्किङ, यातायात लगायतका विशिष्ट क्षेत्रहरू पहिचान गरिएका छन्। यस प्रकारको स्पष्टता सूचना प्रविधि र साइबर सुरक्षा विधेयकमा पनि आवश्यक छ।

सुझाव:

- 'संवेदनशील सूचना संरचना'को स्पष्ट र पारदर्शी परिभाषा विधेयकमा समावेश गर्नुपर्छ।
- सरकारले "संवेदनशील सूचना संरचना" क्षेत्रहरू पहिचान गर्न जोखिम मूल्याङ्कन प्रक्रिया सञ्चालन गरी सोको निष्कर्ष प्रकाशन गर्नुपर्छ।
- कानुनको व्यापक दायरा नहुने कुरा सुनिश्चित गर्न सो मूल्याङ्कन प्रतिबिम्बित हुने गरी दफा ५४ लाई अद्यावधिक गर्नुपर्छ।
- "संवेदनशील सूचना पूर्वाधारको चौबिसै घण्टा अनुगमन गर्ने तथा" हटाउनुपर्छ।

४. प्रविधिको प्रयोग गरी गरिने लैङ्गिक हिंसा सम्बन्धी कसुर र सजाय सम्बन्धी कानुनी मौनता

यस विधेयकले प्रचलित विद्युतीय कारोबार ऐनलाई खारेज गर्नेछ। विधुतिय कारोबार ऐनलाई साइबर अपराध सम्बन्धी पर्याप्त व्यवस्था नभएको कारणले विशेषतः प्रविधिको प्रयोग गरी गरिने लैङ्गिक हिंसा, cyber stalking, Cyber bullying, sextotion, extortion जस्ता अपराध सम्बोधन नगरेकै कारण समयानुकूल परिमार्जन आवश्यक रहेको स्वीकार गरिएको हो। सरकारले पटक- पटक नयाँ कानुनको आवश्यकता औंल्याउँदै त्यस्ता प्रविधिको प्रयोग गरी गरिने लैङ्गिक हिंसा सम्बोधन गर्नुपर्ने आवश्यकता रहेको तर्क दिएको भए पनि, यस विधेयकले प्रविधिको प्रयोगगरि गरिने सम्बोधन गर्ने कुनै प्रावधान समावेश गरेको छैन।

सुझाव:

प्रविधिको प्रयोग गरी गरिने लैङ्गिक हिंसा, cyber stalking, Cyber bullying, sextotion, extortion जस्ता अपराध सम्बोधन सम्बन्धी प्रावधानको प्रस्ट व्यवस्था हुनु पर्ने।

५. डोमेन नाम दर्ता, व्यवस्थापन र नियमन सम्बन्धी व्यवस्था

यस विधेयकको परिच्छेद ५ ले डोमेन नाम, दर्ता तथा व्यवस्थापन सम्बन्धी व्यवस्था गरेको छ, जसमा दफा ३९ ले सूचना तथा प्रविधि विभागलाई डोमेन नाम, सोको व्यवस्थापन तथा नियमनको जिम्मेवारी दिएको छ। यस दफाको प्रावधान अनुसार सबै डोमेनको व्यवस्थापन र नियमन विभागले गर्ने देखिन्छ। नेपालको उच्च डोमेन (Country Code Top Level Domain– ccLTD) विभागले व्यवस्थापन र नियमन गर्ने सक्ने भएता पनि अन्य टप लेवल डोमेन जस्तै .com, .org .net आदिको दर्ता, व्यवस्थापन र नियमन विभागले गर्ने मिल्ने र गर्न सक्ने कुरा होइन। यसरी हेर्दा दफा ३९ को व्यवस्था निकै बृहत् रहेको छ, जसलाई .np (डट एनपी) डोमेन मात्र समेट्ने गरी स्पष्ट बनाउनु पर्ने देखिन्छ।

त्यस्तै दफा ३९ (२) मा विभागले डोमेन नाम सञ्चालकलाई आवश्यक निर्देशन दिन सक्नेछ भन्ने व्यवस्था गरिएको छ भने दफा ४० (१) एनपी डोमेनमा नाम दर्ता गराँउदा विभागले तोकेको संस्थामा दर्ता गराउनुपर्ने भन्ने व्यवस्था छ। तर यस विधेयकमा कतै पनि डोमेन नाम सञ्चालक को हुनेछ, विभागले डोमेन नाम दर्ता गर्ने संस्था कुन प्रक्रिया र मापदण्डका आधारमा तोक्ने वा छनौट गर्नेछ, डोमेन नाम सञ्चालकको छनौट प्रतिस्पर्धात्मक हुने छ वा छैन, हाल संचालनमा रहेको .np डोमेन नाम प्रणालीका सम्बन्धमा के हुनेछ भन्ने बारेमा कुनै पनि स्पष्टता छैन।

त्यसै गरी दफा ४१ ले सुरक्षित रहेका डोमेन नामहरूका बारेमा व्यवस्था गरेको छ, जसअन्तर्गत भौगोलिक तथा पर्यटकीय स्थलका नाम, पुरातात्त्विक तथा धार्मिक महत्त्वका नामका साथसाथै नेपाल सरकारले तोकेका अन्य नाम समेत दोस्रो तथा तेस्रो तहका डोमेन नामका लागि सुरक्षित सूचिमा छन् । यस्तो व्यवस्थाले वैध प्रयोगकर्ताको स्वतन्त्रतालाई सीमित बनाउँछ भने अभिव्यक्ति स्वतन्त्रता र व्यापारिक स्वतन्त्रतामा समेत असर पार्दछ ।

उदाहरणका लागि पोखरामा व्यापार गर्ने कुनै व्यापारिक प्रतिष्ठानले www.visitpokhara.com.np दर्ता गर्न चाहेमा यो विधेयकले तोकेको 'भौगोलिक तथा पर्यटकीय स्थलका नाम' अन्तर्गतको सुरक्षित नाम अन्तर्गत पर्‍यो भनी खारेजीमा पर्न सक्छ । प्रत्येक त्यस्ता नामका लागि मन्त्रालयमा स्वीकृतिका लागि जानुपर्ने हुन्छ । यो व्यवस्था अनावश्यक र अव्यवहारिक छ ।

त्यसै गरी विधेयकको दफा ४१(३) मा सुरक्षित नामसँग मिल्दोजुल्दो हुने गरी वा उक्त नामको महत्त्वलाई अवमूल्यन हुने गरी डोमेन नाम दर्ता गर्न गराउन हुँदैन भन्ने उल्लेख छ तर त्यसो गरेमा के हुन्छ भन्ने सम्बन्धमा कुनै व्यवस्था गरिएको छैन । साथै विधेयक डोमेनमा कसको अधिकार हुने भन्ने सम्बन्धमा कुनै विवाद आएमा त्यसको समाधान कसरी गरिनेछ भन्ने सम्बन्धमा पनि केही उल्लेख गरेको छैन ।

उल्लेखित प्रावधानहरूको विश्लेषण गर्दा विधेयकमा प्रस्ताव गरिएको डोमेन नाम सम्बन्धी प्रावधानहरू अस्पष्ट, अपर्याप्त र अपुरो रहेको र यसले अभिव्यक्ति स्वतन्त्रता र व्यापारिक स्वतन्त्रतामा समेत असर पार्ने देखिन्छ ।

सुझाव:

दफा ३५ को दायरा स्पष्ट पार्नुपर्ने: .com, .org, .net जस्ता अन्तर्राष्ट्रिय टप लेभल डोमेनहरूको दर्ता, व्यवस्थापन र नियमन नेपाल सरकार वा विभागको अधिकार क्षेत्रमा नपर्ने हुनाले उक्त दफा केवल नेपालको उच्च डोमेन (.np) सम्म सीमित हुने गरी स्पष्ट शब्दमा प्रावधान राखिनुपर्छ ।

डोमेन नाम सञ्चालक: विधेयकमा डोमेन नाम सञ्चालक को हुने, कुन मापदण्डका आधारमा छनोट गर्ने, चयन प्रतिस्पर्धात्मक हुने वा नहुने, र हालको .np डोमेन सञ्चालन प्रणालीको भविष्य के हुने भन्ने विषय स्पष्ट पारिनुपर्छ ।

सुरक्षित सूची: दफा ४१ मा राखिएका भौगोलिक, पर्यटकीय, पुरातात्त्विक, धार्मिक नामहरूलाई अत्यधिक प्रतिबन्धात्मक तरिकाले सुरक्षित सूचीमा राख्दा वैध प्रयोगकर्ता, व्यावसायिक स्वतन्त्रता र अभिव्यक्ति स्वतन्त्रता सीमित हुने भएकाले यस सूचीलाई सीमित र व्यावहारिक बनाउने व्यवस्था बनाउनु पर्छ र सुरक्षित सूचीमा पर्ने प्रत्येक नामका लागि मन्त्रालयमा अनिवार्य स्वीकृति लिनुपर्ने प्रावधानलाई हटाएर, स्वतन्त्र र सहज दर्ता प्रक्रिया सुनिश्चित गर्नुपर्ने ।

विवाद समाधान: दफा ४१(३) अन्तर्गत सुरक्षित नामसाग मिल्दोजुल्दो नाम दर्ता गर्न नपाउने प्रावधानको उल्लङ्घन भएमा के कारवाही वा प्रक्रिया हुनेछ भन्ने कुरा विधेयकमा स्पष्ट गर्नु पर्छ, र डोमेन अधिकारसम्बन्धी विवाद उत्पन्न भएमा समाधानका लागि स्पष्ट कानुनी प्रक्रिया, निकाय वा मध्यस्थता संयन्त्रको प्रावधान राखिनुपर्ने ।

६. सेवा प्रदायक सम्बन्धी व्यवस्था

क) सेवा प्रदायकको सङ्कुचित परिभाषा

विधेयकको दफा २ (कघ) ले सेवा प्रदायक भन्नाले कुनै तेस्रो पक्षसँगको सम्झौता बमोजिम सूचना आदानप्रदान वा भण्डारण गर्ने डाटा सेन्टर, क्लाउड सेवा वा सोही प्रकृतिको अन्य सेवा प्रदायक सम्झनु पर्छ भनी परिभाषित गरेको छ । तर यो परिभाषा निकै संकुचित रहेको छ । सूचना प्रविधिको हकमा हुने सेवा प्रदायकहरू डाटा सेन्टर, क्लाउड सेवा वा सोही प्रकृतिको मात्र नभई अन्य जस्तै टेलिकम सेवा प्रदायक, इन्टरनेट सेवा प्रदायक, नेटवर्क सेवा प्रदायक, होस्टिङ सेवा प्रदायक, डोमेन सेवा प्रदायक सबै पर्ने र सो को प्रकृति पनि फरक हुने हुँदा अन्य सेवा प्रदायकलाई समेत समेट्ने गरी हालको परिभाषालाई परिमार्जन गरिनुपर्ने देखिन्छ ।

सुझाव:

इन्टरनेट सेवा प्रदायक, नेटवर्क सेवा प्रदायक, होस्टिङ सेवा प्रदायक, डोमेन सेवा प्रदायक लगायतका अन्य सेवा प्रदायक लाई पनि समेटिनु पर्छ ।

ख) सेवा प्रदायकको दायित्व सम्बन्धी व्यवस्था (मध्यस्थकर्ताको जिम्मेवारी)

विधेयकको दफा ६४ (१) मा सेवा प्रदायकले दायित्व व्यहोर्नु नपर्ने भन्ने व्यवस्था गरी 'कुनै तेस्रो पक्षको सूचना वा तथ्याङ्क वा लिङ्कमा पहुच उपलब्ध गराएको कारणबाट मात्र उक्त सूचना वा तथ्याङ्क वा लिङ्कमा उल्लेख वा समावेश भएको कुनै तथ्य वा विवरणको सम्बन्धमा उत्पन्न हुने कुनै दायित्व व्यहोर्नु नपर्ने' व्यवस्था गरिएको छ ।

तर सोही दफाको उपदफा २ मा 'उपदफा (१) मा जुनसुकै कुरा लेखिएको भए तापनि कुनै सूचना, तथ्याङ्क वा लिङ्कमा उल्लेख वा समावेश भएको कुनै तथ्य वा विवरणले प्रचलित कानुनको उल्लङ्घन गरेमा वा कुनै गैरकानुनी कार्य गर्न दुरुत्साहन वा सहयोग गरेमा सेवा प्रदायक त्यस्तो दायित्वबाट मुक्त हुने छैन' भन्ने व्यवस्था गरी उपदफा १ को संरक्षणलाई प्रभावहीन बनाइएको छ । यो व्यवस्था मध्यस्थ जिम्मेवारीको अपवादको उद्देश्य विपरीत छ, किनकि अपवादको उद्देश्य नै सेवा प्रदायकको प्याल्टफर्ममा प्रकाशित तेस्रो पक्ष सामग्री अवैध रहेछन् भने सेवा प्रदायकहरूलाई सो को जिम्मेवारीबाट मुक्त गर्नु हो ।

कुनै गैरकानुनी कार्य गर्न दुरुत्साहन वा सहयोग गरेमा सेवा प्रदायक त्यस्तो दायित्वबाट मुक्त नहुने व्यवस्था कानुन र सर्वमान्य सिद्धान्त बमोजिम नै भएता पनि कुनै सूचना, तथ्याङ्क वा लिङ्कमा उल्लेख वा समावेश भएको कुनै तथ्य वा विवरणले प्रचलित कानुनको उल्लङ्घन गरेमा पनि दायित्व व्यहोर्नुपर्ने व्यवस्थाले तेस्रो पक्षद्वारा पहुँच गरिएका अवैध सामग्रीको लागि सेवा प्रदायकहरूलाई आपराधिक रूपले जिम्मेवार ठहराउने व्यवस्था भएको छ । यसले सेवा प्रदायकहरूलाई अनावश्यक जोखिममा पार्छ र स्वतन्त्र इन्टरनेटको अवधारणालाई जोखिममा पार्छ ।

त्यसै गरी दफा ६४ (१) (घ) मा यदि सेवा प्रदायकले 'सम्बन्धित नियामक निकायको निर्देशन पालना गरेको भएमा दायित्व व्येहोर्नु नपर्ने' भन्ने व्यवस्था गरिएको छ । सेवा प्रदायकले सम्बन्धित नियामक निकायको निर्देशन पालना गर्ने दायित्व निजले पाउने अनुमति पत्र अन्तर्गत व्यवस्थित गरिनुपर्ने विषय भएको, कस्तो प्रकृतिको निर्देशन हो भन्ने स्पष्ट नभएकाले यो प्रावधानलाई यस दफाबाट हटाइनुपर्छ । यदि सामग्री हटाउने सम्बन्धमा दिइएको निर्देशन हो भने त्यो विषय स्पष्ट रूपमा उल्लेख गरिनुपर्छ । यसरी अस्पष्ट रूपमा उल्लेख गरिनुहुँदैन ।

सुझाव:

तेस्रो पक्षद्वारा पहुँच गरिएका अवैध सामग्रीका सम्बन्धमा सेवा प्रदायकलाई जानकारी नभएका अवस्थामा र निजको स्वैच्छिक सहभागिता नभएका अवस्थामा सेवा प्रदायकहरूलाई आपराधिक रूपले जिम्मेवार ठहराउनु हुँदैन । प्रस्तावित प्रावधानमा संशोधन गरिनुपर्छ ।
त्यसै गरी यदि नियामक निकायको निर्देशन भनी सेवा प्रदायकलाई सामग्री हटाउनका लागि दिइने निर्देशन भन्न खोजिएको हो भने त्यो विषय स्पष्ट रूपमा उल्लेख गरिनुपर्छ । त्यस्तो अवस्थामा अदालतको आदेश अनिवार्य रूपमा आवश्यक पर्ने व्यवस्था गरिनुपर्छ र त्यस्ता सामग्री हटाउने निर्देशनका विरुद्ध स्वतन्त्र, निष्पक्ष न्यायालय वा न्यायिक निकाय समक्ष चुनौती दिन पाउने अनिवार्य कानुनी व्यवस्था समेट्ने भाषा समावेश गरिनुपर्छ ।

७. ट्राफिक तथ्याङ्कमा नियन्त्रण र विषयवस्तुमा अन्तरदोहन सम्बन्धी व्यवस्था

क) ट्राफिक तथ्याङ्कमा पहुँच र नियन्त्रण

यस विधेयकको दफा १०६ ले कुनै खास सञ्चारसाग सम्बद्ध ट्राफिक तथ्याङ्क कुनै कसुरको अनुसन्धान प्रयोजनको लागि अदालतले तत्काल प्राप्त प्रमाणको आधारमा आवश्यक ठानेमा अनुसन्धान अधिकृतलाई खास सञ्चार सम्बन्धी ट्राफिक तथ्याङ्कमा पहुँच राख्न अनुमति दिन सक्ने व्यवस्था गरेको छ ।

साथै दफा १०७ (१) ले कुनै खास सञ्चारसँग सम्बद्ध ट्राफिक तथ्याङ्क कुनै कसुरको अनुसन्धान प्रयोजनको लागि अदालतले तत्काल प्राप्त प्रमाणको आधारमा आवश्यक देखेमा उक्त तथ्याङ्कमा नियन्त्रण गर्न २ किसिमको आदेश दिन सक्ने व्यवस्था गरेको छ । तर यस यी दुई दफामा कसुर भन्नाले यसै विधेयक अनुसारको कसुर मात्र हो की अन्य प्रचलित कानुन बमोजिमको अन्य कसुर पनि पर्छ भन्ने प्रस्ट छैन । यसरी ट्राफिक तथ्याङ्कमा पहुँच, नियन्त्रण दिने कसुरको गाम्भिर्यता के कस्तो हो भन्ने पनि स्पष्ट छैन । गम्भीर कसुरसम्बन्धी अन्य प्रचलित कानुनजस्तै मानव बेचबिखन, सङ्गठित अपराध जस्ता कानुनमा आवश्यकता अनुसार अदालतको आदेशमा विद्युतीय तथ्याङ्क पहुँच, सङ्कलन वा अभिलेखन गर्न सक्ने व्यवस्था भएकोमा यो व्यवस्था यस आवश्यक छ कि छैन भन्नेमा पुनर्विचार गर्नु पर्ने देखिन्छ ।

साथै दफा १०७ (१) मा उल्लेख गरिएको 'नियन्त्रण गर्ने' भन्ने व्यवस्था अस्पष्ट, वृहत् र आवश्यकतामा आधारित छैन र यसले नागरिकको गोपनीयता सम्बन्धी अधिकारको उल्लङ्घन गर्दै व्यापक दुरुपयोगको जोखिम सिर्जना गर्दछ ।

सुझाव:

- दफा १०६ र १०७ मा "कसुर" भन्नाले कुन-कुन कसुरलाई जनाउने हो भन्ने कुरा स्पष्ट परिभाषित हुनुपर्छ (यसै विधेयकमा उल्लेखित कसुर कि अन्य प्रचलित कानुनमा रहेका गम्भीर कसुर समेत) भन्ने प्रस्टीकरण आवश्यक छ ।
- "गम्भीर कसुर" (जस्तै मानव बेचबिखन, सङ्गठित अपराध, आतङ्कवाद सम्बन्धी अपराध) मात्रका लागि ट्राफिक तथ्याङ्कमा पहुँच वा नियन्त्रण दिने व्यवस्था गर्नुपर्छ, ताकि सामान्य वा साना कसुरका लागि निजताको हक अकारण उल्लङ्घन नहोस् ।
- दफा १०७(१) मा प्रयोग गरिएको "नियन्त्रण" शब्द कानुनी दृष्टिले अनौठो (unprecedented) छ । यसले अदालतलाई वा अनुसन्धान अधिकृतलाई नागरिकको सञ्चार प्रणाली वा तथ्याङ्क माथि अत्यधिक अधिकार दिने सम्भावना रहेको हुँदा, यसलाई प्रष्ट परिभाषित गर्नुपर्छ वा हटाउनुपर्छ ।
- यस्ता प्रावधानले TERAMOCS जस्ता निगरानी प्रविधि भित्र्याउने कानुनी आधार दिने भएकाले, यसबाट नागरिकको गोपनीयता र मानव अधिकारमा नकारात्मक असर पर्न सक्ने जोखिम छ । त्यसैले प्रावधान राख्दा गोपनीयता, डाटा सुरक्षा, मानव अधिकार र आनुपातिकताको मापदण्डलाई अनिवार्य रूपमा सुनिश्चित गर्नुपर्छ ।
- त्यस्तै दफा १०७ को उपदफा १ र उपदफा २ मा राखिएको व्यवस्था एउटै भएको हुनाले उपदफा २ हटाउनु पर्ने ।

ख) विषयवस्तुको अन्तरदोहन (इन्टरसेप्सन) सम्बन्धी व्यवस्था

यस विधेयकको दफा १०८ (१) ले सञ्चारको कुनै विषयवस्तु कसुरको अनुसन्धान प्रयोजनको लागि तत्काल प्राप्त प्रमाणको आधारमा अदालतले आवश्यक देखेमा सेवा प्रदायकलाई प्रयोग गरी विद्युतीय प्रणाली मार्फत प्रसार भएको खास सञ्चारको विषयवस्तु प्रसार हुदाहुदैको अवस्थामा सङ्कलन वा अभिलेख गर्न वा अख्तियार प्राप्त अधिकारीलाई सोका लागि अनुमति दिन र सहायता गर्न आदेश गर्न सक्ने व्यवस्था गरेको छ। साथै १०८ (२) ले यसरी सङ्कलन वा अभिलेख गर्न अनुसन्धान अधिकृतलाई अख्तियारी प्रदान गर्न सक्ने व्यवस्था गरेको छ।

यस दफामा उल्लेख गरेको 'कसुर' अन्तर्गत यसै विधेयक अन्तर्गत व्यवस्था गरिएका कसुर मात्र समावेश हुन् की प्रचलित कानुन बमोजिमको अन्य कसुर पनि पर्छ भन्ने प्रष्ट छैन। यसरी विषयवस्तुको अन्तरदोहनमा सङ्कलन वा अभिलेख गर्न वा अख्तियार प्राप्त अधिकारीलाई सोका लागि अनुमति दिन र सहायता गर्न आदेश गर्न सक्ने भनेको कसुरको गम्भिर्यता के कस्तो हो भन्ने पनि स्पष्ट छैन। गम्भीर कसुरसँग सम्बन्धित प्रचलित कानुन, जस्तै मानव बेचबिखन, सङ्गठित अपराध जस्ता कानुनमा आवश्यकता अनुसार अदालतको आदेशमा विषयवस्तुको अन्तरदोहनमा सङ्कलन वा अभिलेख गर्न वा अख्तियार प्राप्त अधिकारीलाई सोका लागि अनुमति दिन र सहायता गर्न आदेश गर्न सक्ने, सङ्कलन वा अभिलेखन गर्न सक्ने व्यवस्था भएकोमा यो व्यवस्था यस आवश्यक छ कि छैन भन्नेमा पुनर्विचार गर्न पर्ने देखिन्छ।

सुझाव:

- दफा १०८ मा "यसै विधेयकमा उल्लिखित कसुर" वा "प्रचलित अन्य कानुनमा परिभाषित गम्भीर कसुर" भन्ने स्पष्टता आवश्यक छ, जसले कानुनको दुरुपयोग वा कानुनी अस्पष्टता नहोस्।
- कुन अवस्थामा सञ्चारको अन्तरदोहन (interception) वा अभिलेख गर्न पाइने हो भन्ने आधार र कसुरको गम्भीरताको तह (गम्भीर/सामान्य) स्पष्ट प्रावधान राखिनुपर्छ।
- निजताको हक र व्यक्तिगत स्वतन्त्रता प्रभावित हुने संवेदनशील विषय भएकाले अदालतको आदेशमा मात्र यस्ता कदम चाल्न सकिने गरी थप सुरक्षा उपाय (safeguards) राखिनुपर्छ।
- दफा १०८ प्रयोग गर्दा अभिलेख वा सङ्कलन गरिएको सूचनाको दुरुपयोग नहोस् भन्ने हेतुले गोपनीयता, डेटा सुरक्षा र उपयोगको सीमा (purpose limitation) स्पष्ट गर्न जरुरी छ।

८. कसुर तथा साइबर अपराधको परिभाषा तथा प्रकारका सम्बन्धमा

साइबर अपराधको परिभाषा र त्यसका लागि सजायको व्यवस्था यस विधेयकको एक मुख्य पाटो हो। तर विधेयकले हालको वास्तविक अवस्थालाई स्पष्ट रूपमा समेट्न सकेको देखिदैन। प्रस्तावित कानुनलाई समयसापेक्ष बनाउन साइवर अपराधहरूको सूची र परिभाषा तयार गर्दा, तिनले नेपाली समाजमा देखिएका वास्तविक प्रवृत्ति, जोखिम र घटनाक्रमलाई प्रतिबिम्बित गर्नुपर्छ। उदाहरणका लागि, हाल नेपालमा इन्टरनेट तथा सामाजिक सञ्जाल दुरुपयोग, अनलाइन लैङ्गिक हिंसा, प्रविधिको प्रयोग गरी गरिने लैङ्गिक हिंसा, डिजिटल ठगी, अनलाइन वित्तीय ठगी, व्यक्तिगत डेटा चोरी, डिजिटल पहिचानको चोरी तथा दुरुपयोग, अनधिकृत पहुच तथा अफवाह फैलाउने कार्यहरूमा व्यापक वृद्धि भएको देखिन्छ। यी प्रवृत्तिहरूलाई ध्यानमा राखेर, प्रावधानहरूलाई व्यावहारिक र कार्यान्वयनयोग्य हुने गरी परिष्कृत गर्नुपर्छ। इन्टरनेट र सामाजिक सञ्जालबाट हुने कसुरका लागि छुटा-छुट्टै कानुन बनाउन आवश्यक नभई यसै कानुनले नै सामाजिक सञ्जाल समेतलाई समेट्ने गरि साइबर अपराध सम्बन्धी कानुन बनाउन सकिन्छ।

साथै यस विधेयकले विभिन्न कसुरहरूको सन्दर्भमा दण्डको उच्चतम सीमा (upper threshold) मात्र उल्लेख गरेको छ। न्यूनतम सीमा (lower threshold) को अभावले न्यायिक विवेकमा अत्यधिक निर्भरता ल्याउन सक्छ, जसले समान प्रकृतिका अपराधमा पनि दण्डमा व्यापक असमानता हुने सम्भावना रहन्छ।

सुझाव:

- अन्तर्राष्ट्रिय मापदण्ड र असल अभ्यासहरूसँग समन्वय गर्दै साइबर अपराधको परिभाषा र कानुन परिष्कृत गर्नु पर्छ इन्टरनेट र सामाजिक सञ्जालमार्फत हुने अपराधहरूलाई यसै विधेयक अन्तर्गत समेट्दै साइबर अपराधका लागि विशेष कानुन बनाउनु पर्ने आवश्यक हुन्छ।
- कसुर र सजाय बीच स्पष्ट अनुपात कायम गर्न न्यूनतम दण्डको सीमा निर्धारण गरिनु पर्ने देखिन्छ।

९. परिभाषामा समावेश हुनु पर्ने व्यवस्था अन्य दफामा राखिएको सम्बन्धमा

विधेयकको स्पष्टता, सुसंगतता र कानुनी प्रभावकारिताका लागि महत्त्वपूर्ण शब्दावलीहरू परिभाषा खण्ड (सामान्यतया दफा २) मा समावेश गरिएको हुन्छ। परिभाषा खण्डमा राखिएका शब्दहरू विधेयकभर एकरूप अर्थमा प्रयोग हुन्छन्, जसले कानुनी व्याख्या गर्दा भ्रम र विवादको सम्भावना कम गर्छ। तर यस विधेयकमा "नवीनतम प्रविधि", "स्रोत कोड", "डिनायल अफ सर्भिस", "फिसिङ्ग" "स्पुफिङ" "इन्टरनेट अफ थिङ्गस" जस्ता महत्वपूर्ण शब्दावलीहरू दफा २ मा नराखी अन्य दफामा स्पष्टीकरणका रूपमा मात्र राखिएको छ, जुन विधेयकको प्रणालीगत संरचना र कार्यान्वयन दुवै दृष्टिले उपयुक्त छैन।

अरू दफामा मात्र राखिँदा यी शब्दहरूको कानुनी दायरा सीमित हुन सक्छ र एउटै शब्द फरक-फरक सन्दर्भमा फरक अर्थमा बुझिने जोखिम रहन्छ । साथै, भविष्यमा प्रविधि र साइबर अपराधसँग सम्बन्धित शब्दावली अद्यावधिक गर्नुपर्ने अवस्थामा, परिभाषा खण्डमा केन्द्रित रहे सजिलो हुन्छ, तर विभिन्न दफामा छरिएको अवस्थामा संशोधन कठिन र असङ्गत बन्न सक्छ । त्यसैले, यस्ता प्राविधिक र विशेष शब्दावलीहरूलाई दफा २ अन्तर्गतको परिभाषा खण्डमै राखी, स्पष्ट, एकरूप र व्यावहारिक कानुनी संरचना सुनिश्चित गर्नुपर्छ ।

सुझाव:

विधेयकको विभिन्न स्थानमा रहेको स्पष्टीकरण खण्डलाई परिभाषा (दफा २) मा समावेश गरिनु उपयुक्त हुन्छ ।

१०. दोहोरो व्यवस्था (Duplication of Legal Provision) र सजायको असन्तुलन (Penalty Mismatch)

यस विधेयकको दफा ८६ मा वैयक्तिक गोपनीयता उल्लङ्घनसम्बन्धी प्रावधान समावेश गरिएको छ, जुन विषय गोपनीयता सम्बन्धी ऐन, २०७५ को दफा १९ उपदफा (२) र (३) मा पहिले नै व्यवस्था गरिसकिएको छ । यी दुवै कानुनमा 'कसैले यस ऐन विपरीत विद्युतीय माध्यमबाट कसैको वैयक्तिक विवरण सङ्कलन गरेमा वा सूचना, जानकारी अनधिकृत रूपमा प्राप्त गर्न, त्यसको गोपनीयता भङ्ग गर्न वा अनधिकृत रूपमा कसैलाई उपलब्ध गराउन हुँदैन' भन्ने व्यवस्था र 'कसैले पनि कुनै दुई वा दुईभन्दा बढी व्यक्तिहरू बिचमा विद्युतीय माध्यमबाट भएका कुनै संवाद वा कुराकानी सङ्केत सम्बन्धित व्यक्तिले मन्जुरी दिएको वा कानुन बमोजिम अधिकार प्राप्त अधिकारीले आदेश दिएकोमा बाहेक कुनै यान्त्रिक उपकरणको प्रयोग गरी सुन्न वा त्यस्तो कुराको ध्वनि अङ्कन वा रेकर्ड गर्न वा गराउन हुदैन' भन्ने व्यवस्था समान रूपमा गरिएको छ ।

यस प्रकारको दोहोरो कानुनी व्यवस्था (overlap) ले कानुनको प्रभावकारिता, व्याख्या र कार्यान्वयनमा अन्योल उत्पन्न गर्नुका साथै विधायनको दृष्टिले पनि आवश्यकताभन्दा बढी पुनरावृत्ति सिर्जना गर्दछ । गोपनीयता सम्बन्धी छुट्टै विशिष्ट ऐन (Privacy Act) विद्यमान रहेको अवस्थामा, सोही विषयवस्तुलाई सूचना प्रविधि सम्बन्धी विधेयकमा पुनः समावेश गर्नु विधायनको स्पष्टताको दृष्टिले उपयुक्त हुँदैन ।

यसै सन्दर्भमा, यस सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धी विधेयकले उल्लङ्घनको प्रकृति र गम्भीरताअनुसार अधिकतम दुई वर्ष कैद वा अधिकतम तीन लाख रुपैयाँ जरिवाना वा दुवै सजायको व्यवस्था गरेको छ । तर, वैयक्तिक गोपनीयता सम्बन्धी ऐन, २०७५ ले सोही उल्लङ्घनका लागि अधिकतम तीन वर्ष कैद वा अधिकतम तीस हजार रुपैयाँ जरिवाना वा दुवै सजायको व्यवस्था गरेको छ । दुवै कानुनले एउटै प्रकारको कार्यलाई गैर कानुनी ठहर गरे तापनि, तिनले तोकेको सजायको सीमा र स्वरूप फरक-फरक छ । यस्तो असमानता र असङ्गतिले कानुन कार्यान्वयनमा स्वविवेकाधिकार दुरुपयोगको सम्भावना बढाउने, एकै प्रकारको अपराधमा फरक दण्ड सजाय हुने अवस्था सिर्जना गर्ने र न्यायिक स्पष्टता तथा निष्पक्षताको सिद्धान्तसाग प्रत्यक्ष रूपमा बाझिने जोखिम रहन्छ ।

सुझाव:

गोपनीयताका सम्बन्धमा यस विधेयकमा समावेश केही प्रावधानहरू गोपनीयता सम्बन्धी विशेष कानुनमा नै समावेश भइसकेकाले यस सम्बन्धमा यस विधेयकमा थप व्यवस्था गरिरहनु पर्दैन ।

निष्कर्ष

हाल संसदमा विचाराधीन सूचना प्रविधि तथा साइबर सुरक्षा विधेयकले प्रविधिको विकास, प्रवर्द्धन र नियमन, विद्युतीय अभिलेख तथा डिजिटल हस्ताक्षरको प्रमाणीकरण, साइबर स्पेसमा सूचना तथा तथ्याङ्कको संरक्षण, साथै प्रचलित कानुनको संशोधन र एकीकरण गर्ने महत्त्वपूर्ण उद्देश्य राखेको छ।

तर, विधेयकमा निहित अस्पष्ट परिभाषा, दोहोरो कानुनी व्यवस्था, तथा अभिव्यक्ति स्वतन्त्रता र डाटा सुरक्षासम्बन्धी व्यापक, तर अस्पष्ट र अपुरो प्रावधानहरूका कारण यसको उद्देश्य र संवैधानिक आधारबारे गम्भीर प्रश्न देखिन्छ। विशेषतः, 'अश्लील सामग्री', 'संवेदनशील सूचना पूर्वाधार', 'सेवा प्रदायक' डोमेन व्यवस्थापन ट्राफिक तथ्याङ्क र विषयवस्तु अन्तरदोहनसम्बन्धी प्रावधानहरू स्पष्ट छैनन् । त्यस्तै, तथ्यांकधारकका अधिकार, उजुरी प्रक्रिया, र क्रस-बोर्डर डाटा स्थानान्तरणसम्बन्धी विषय पर्याप्त रूपमा समेटिएका छैनन् ।

विधेयकलाई स्पष्ट, नागरिक-मुखी, मानव अधिकारमैत्री र सूचना प्रविधि विकास अनुकूल बनाउन, सरोकारवालासाग व्यापक परामर्श र छलफल अनिवार्य छ। यसका लागि, विधेयक संसदबाट पारित हुनु अघि कानुनी स्पष्टता, अधिकार र स्वतन्त्रताको सन्तुलन, तथा प्रविधि विकासलाई प्रोत्साहित गर्ने प्रावधानहरू समावेश हुने गरी आवश्यक संशोधन गरिनु आवश्यक छ।

डिजिटल राइट्स नेपाल यस प्रक्रियामा सरोकारवालासँग रचनात्मक सहकार्य र साझेदारीका लागि प्रतिबद्ध छ।

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 प्रवर्द्धन 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.digitalrightsnepal.org मा जानुहोस् ।

Digital Rights Nepal

Phone: +977-9767245100
Address: 47 - Neel Saraswoti Marga, Gairidhara - 2, Kathmandu
Email: info@digitalrightsnepal.org
Web: www.digitalrightsnepal.org