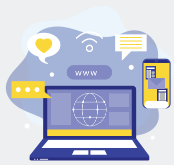
राष्ट्रिय साइबर सुरक्षा नीति २०८०

नेपालमा मानव अधिकारका तीन चुनौती

राष्ट्रिय साइबर सुरक्षा नीति २०८० (नीति) ले नेपाललाई साइबर आक्रमणबाट जोगाउने र इन्टरनेटलाई सुरक्षित राख्ने लक्ष्य राखेको छ। यस नीतिले यो लक्ष्य प्राप्त गर्न सरकारले चाल्नुपर्ने आवश्यक कदमहरुको व्याख्या गर्दछ। नीतिका धेरै पक्षहरू सकारात्मक रहेको तथा यसले साइबर सुरक्षालाई बलियो बनाउने भए तापनि यसका केही प्रावधानहरुले मानव अधिकारमा नकारात्मक असर पार्न सक्छन्।[1]

डिजिटल राइट्स नेपाल (डिआरएन) र इन्टरनेशनल सेन्टर फर नट-फर-प्रोफिट ल (आइसिएनएल) ले यस नीतिमा रहेका तीन वटा प्रमुख मानवअधिकार सम्बन्धी सरोकारहरूको बारेमा मन्त्रालयका अधिकारी, विधायक तथा नागरिक समाजलाई जानकारी गराउन यो संक्षिप्त पत्र तयार पारेको छ:



राष्ट्रिय इन्टरनेट गेटवे:

यस नीतिले नेपालबाट भित्र र बाहिर हुने सबै इन्टरनेट ट्राफिकहरूलाई व्यवस्थापन गर्न राष्ट्रिय इन्टरनेट गेटवे (एनआइजी) (दफा ११.२५) स्थापना गर्न सरकारलाई आह्वान गरेको छ। अनलाइन जानकारी नियन्त्रण गर्न र व्यक्तिको व्यक्तिगत सञ्चारको निगरानी गर्न यो सरकारको लागि एक शक्तिशाली उपकरण बन्न सक्छ।

अनलाइन अभिव्यक्ति स्वतन्त्रता तथा सामग्री प्रकाशनमा गम्भीर प्रतिबन्धहरू:

यस नीतिले सरकारलाई मन नपर्ने कुनै पनि प्रकारको अभिव्यक्तिलाई प्रतिबन्ध लगाउन तथा निषेध गर्न सक्षम बनाउँछ। सरकारलाई धेरै साँघुरो र सीमित अवस्थामा मात्र अभिव्यक्ति स्वतन्त्रतामा प्रतिबन्ध लगाउने अधिकार हुनुपर्नेमा यस नीतिले वृहत्, अस्पष्ट, र परिभाषित नगरिएका अभिव्यक्तिहरूलाई निषेध गर्न आह्वान गर्दछ।

अनलाइन अभिव्यक्ति र गतिविधिहरूको नियमित अनुगमन:

यस नीतिले अनलाइन स्पेसको "नियमित अनुगमन" गर्न सरकारलाई आह्वान गरेको छ। यो आफैमा अनुपयुक्त व्यवस्था होइन, तर अभिव्यक्ति स्वतन्त्रता र गोपनीयताको अधिकारलाई प्रतिबन्धित नगर्ने सुनिश्चित गर्न सशक्त प्रत्याभूतिहरूको व्यवस्था गरिनुपर्छ।

साइबर सुरक्षा र मानव अधिकार परस्पर अन्तर्विरोधी हैनन्। प्रभावकारी साइबर सुरक्षा संरचनाका लागि सशक्त मानव अधिकार संरक्षण अत्यावश्यक छ। मन्त्रालयका अधिकारीहरू, संसद सदस्य लगायत सरकारले, तल उल्लेख गरिएका सरोकारहरूलाई सम्बोधन गर्दै मानव अधिकारको रक्षा गर्ने र साइबर सुरक्षाका उत्कृष्ट अभ्यासहरू अनुसरण गर्ने कानुन तथा नीति नियमहरू बनाउनका लागि नागरिक समाजसँग मिलेर काम गर्नुपर्छ।

---

[1] उदाहरणका लागि, दफा ११.१८ ले अन्तर्राष्ट्रिय असल अभ्यासहरूसँग मेलखाने गरी सूचना सञ्चार प्रणाली तथा सेवाहरू बीचको डाटा आदानप्रदानमा इन्क्रिप्शनको प्रयोगलाई अनिवार्य गर्दछ। यसले कानून प्रवर्तन प्रयासहरूमा सम्झौता नगरी गोपनीयता र सुरक्षा सुनिश्चित गर्दछ। त्यसै गरी, दफा ११.५ ले नेपालको अन्तर्राष्ट्रिय कानुनी दायित्व तथा लोकतान्त्रिक मूल्यमान्यतालाई परिपालना गर्नुपर्ने कुराको महत्वलाई जोड दिँदै मौलिक अधिकारसम्बन्धी अन्तर्राष्ट्रिय मापदण्डहरू अनुसार कानुनी र नीतिगत उपायहरूको आवश्यकताको बारेमा व्यवस्था गरेको छ। यसको साथै, दफा ११.५१ देखि ११.५५ ले ज्येष्ठ नागरिक, महिला, बालबालिका र विशेष आवश्यकता भएका व्यक्तिहरू जस्ता जोखिम समूहहरूलाई विशेष ध्यान दिई साइबर सुरक्षासम्वन्धी जनचेतना अभियानको आवश्यकतासम्वन्धी व्यवस्था गरेको छ।

यसको किन महत्व छ ?

निःशुल्क र खुला इन्टरनेट प्राविधिक आविष्कार मात्र होइन, यो समसामयिक लोकतन्त्रको आधारशिला हो र अभिव्यक्ति स्वतन्त्रता तथा गोपनीयताको अधिकार सहित मौलिक मानवअधिकारको उपयोग गर्ने एउटा महत्त्वपूर्ण माध्यम हो । विश्वव्यापी रुपमा जोडिएको यस समाजमा इन्टरनेट सञ्चार, सूचना आदान प्रदान र नागरिक सहभागिताको लागि प्राथमिक माध्यम हो । यसले व्यक्तिहरूलाई आफ्ना विचारहरू व्यक्त गर्न, विविध विचारहरू आदानप्रदान गर्न र महत्वपूर्ण विषयवस्तु सम्बन्धी सार्वजनिक संवादमा भाग लिन सक्षम बनाउँछ ।

डिजिटल स्पेसमा मानव अधिकारको संरक्षण गर्नका लागि यी सिद्धान्तहरूलाई परिपालना गर्नु आवश्यक छ । व्यक्तिहरूले स्वतन्त्र तथा सुरक्षित रूपमा आफ्नो अधिकारलाई अनलाइनमा उपयोग गर्न पाएको प्रत्याभूति गर्न सावधानीपूर्वक तयार गरिएको साइबर सुरक्षा कानून अत्यावश्यक छ ।

राष्ट्रिय साइबर सुरक्षा नीति २०८० मा नै कानुन तथा नीति नियमहरूले मौलिक अधिकारहरूसँग सम्बन्धित अन्तर्राष्ट्रिय मापदण्डहरू परिपालना गर्नुपर्छ भनी उल्लेख गरिएको छ । नीतिको दफा ११.५ ले साइबर सुरक्षा सम्बन्धी कानून तथा नीति नियमहरूको निर्माणमा अन्तर्राष्ट्रिय मापदण्डहरू कायम राख्ने प्रतिबद्धता गरेको छ ।[२]

यस नीतिले साइबर सुरक्षा मात्र नभई डिजिटल क्षेत्रमा स्वतन्त्रता तथा सुरक्षा लगायतका विश्वव्यापी मूल्यमान्यताहरूलाई सक्रिय रूपमा प्रवर्द्धन तथा अभिवृद्धि गर्ने महत्वपूर्ण अवसर प्रदान गर्दछ । व्यक्तिहरूले स्वतन्त्र तथा सुरक्षित रूपमा आफ्ना अधिकारहरू अनलाइनमा प्रयोग गर्न पाउने कुराको सुनिश्चितता गरी नीतिले थप समावेशी तथा सहभागितामूलक डिजिटल वातावरणलाई बढवा दिन्छ । स्वतन्त्रतामा कटौती गर्नुको सट्टा यस नीतिले व्यक्तिहरूलाई डिजिटल स्पेसहरूमा अर्थपूर्ण रूपमा संलग्न हुन सशक्त बनाउन उत्प्रेरकको रूपमा काम गर्न सक्छ, जसले लोकतान्त्रिक सिद्धान्तहरूलाई बलियो तथा सुदृढ बनाई नेपालको डिजिटल स्पेस/परिदृश्यमा मानव अधिकारलाई प्रवर्द्धन गर्छ ।

[२] दफा ११.५: सूचनाको हक तथा गोपनियताको हक एवं मौलिक हकहरुको संरक्षणसम्वन्धी राष्ट्रिय, क्षेत्रिय तथा अन्तर्राष्ट्रिय मापदण्डहरु अनुसार कानूनी तथा नीगिगत उपायहरु अवलम्वन गरिने ।

राष्ट्रिय साइबर सुरक्षा नीतिमा रहेका तीन मुख्य सरोकारहरु:

१ राष्ट्रिय इन्टरनेट गेटवे

के हो राष्ट्रिय इन्टरनेट गेटवे ?

राष्ट्रिय इन्टरनेट गेटवे (एनआइजी) भनेको कुनै देशमा प्रवेश गर्ने र बाहिरिने सबै इन्टरनेट ट्राफिकको लागि केन्द्रीय चेकपोइन्ट हो । सामान्यतया, देशहरूको इन्टरनेट धेरै बिन्दुहरू भई विश्वका अरु देशहरुसँग जोडिन्छन् । तर एनआइजी राखिएमा सबै इन्टरनेट ट्राफिक सरकारद्वारा नियन्त्रित एकल बिन्दु मार्फत देश भित्र(बाहिर जान्छ । अर्को शब्दमा एनआइजी राखिनुको अर्थ धेरै साना गेटहरूको सट्टा एउटा मुख्य गेट राखिए जस्तै हो ।

एनआइजी किन महत्वपूर्ण छ? सबै इन्टरनेट ट्राफिकको लागि एउटा केन्द्रीय बिन्दु हुनुले सरकारलाई अनलाइनमा के भइरहेको छ भनेर निगरानी राख्न धेरै सजिलो हुन्छ । यसले गर्दा वेबसाइट वा सूचना निगरानी, फिल्टर वा ब्लक गर्न सजिलो हुन्छ । यसले देशको इन्टरनेटमार्फत के भित्र आइरहेको छ वा के बाहिर गइरहेको छ भनी हेर्ने ठुलो सुरक्षा क्यामेरा जस्तो काम गर्छ ।

यसले साइबर सुरक्षामा मद्दत गर्न सक्ने भए तापनि गोपनीयता र अभिव्यक्तिको स्वतन्त्रतामाथि जोखिम थप्छ ।[३] यदि सबै इन्टरनेट ट्राफिक एउटै गेटबाट जान्छ भने, सरकारले सम्भावित रूपमा मानिसहरूले अनलाइन के गरिरहेका छन् भनेर हेर्न र नियन्त्रण गर्न सक्छ । यस कारण यो व्यवस्था गोपनीयता तथा अभिव्यक्ति स्वतन्त्रता जस्तो आम नागरिकको अधिकारको लागी एक महत्वपूर्ण खतरा हो ।

मानव अधिकारसम्बन्धी खतराहरु के के छन् ?

प्रतिबन्ध (सेन्सरसिप)को जोखिम/अभिव्यक्तिको स्वतन्त्रतामाथि खतरा: एनआइजीको कार्यान्वयनले अभिव्यक्ति स्वतन्त्रताको मौलिक अधिकारलाई खतरामा पार्नुको साथै प्रतिबन्ध (सेन्सरसिप)को ठुलो जोखिम निम्त्याउन सक्छ । एकल केन्द्रीकृत बिन्दु मार्फत सबै इन्टरनेट ट्राफिकलाई पठाउने गर्दा सरकारले सूचनाको प्रवाहमा व्यापक नियन्त्रण कायम गरी आफ्नो एजेन्डा/स्वार्थ अनुसार अनलाइन सामग्रीलाई नियमन र प्रतिबन्ध (सेन्सर) गर्न सक्छ । यस प्रकारका केन्द्रीकृत नियन्त्रणले अधिकारीहरूलाई वेबसाइटहरू, प्लेटफर्महरू वा आलोचनात्मक वा अवाञ्छित मानिने सामग्रीहरूमा पहुँच रोक्न, असहमति जनाउने विचारहरूलाई दबाउन र सार्वजनिक बहसहरु सीमित गर्ने अनुमति दिन्छ । यस्तो प्रतिबन्ध (सेन्सरसिप)ले स्वस्थ लोकतन्त्रको लागि आवश्यक विचारहरूको प्रभावकारी आदानप्रदान तथा दृष्टिकोणको विविधतालाई कमजोर बनाउँछ, वाक स्वतन्त्रताको जगमा असर पार्दछ र प्रतिशोधको डरबिना स्वतन्त्र रूपमा अनलाइनमा अभिव्यक्ति गर्ने नागरिकहरूको क्षमतालाई कमजोर बनाउँछ ।

निगरानी/गोपनीयताको लागि खतरा: एनआइजीले इन्टरनेट ट्राफिकका व्यापकरुपमा निगरानी गर्ने क्षमता अभिवृद्धि गरी गोपनीयता अधिकारमा महत्वपूर्ण खतरा बढाउँछ । एकल बिन्दु मार्फत सबै इन्टरनेट ट्राफिक पठाई, सरकारले ब्राउजिङ्ग इतिहास, सञ्चार र अनलाइन गतिविधिहरू सहित व्यक्तिगत डाटामा पहुँच प्राप्त गर्दछ । यस्तो व्यापक निगरानीले व्यक्तिहरूको गोपनीयताको अधिकारलाई उल्लङ्घन गर्छ, किनकि यसले अधिकारीहरूलाई नागरिकहरूको सहमति वा जानकारी बिना उनीहरुको अनलाइन व्यवहार निगरानी गर्ने र ट्र्याक गर्ने अनुमति दिन्छ । संवेदनशील व्यक्तिगत डाटाको सङ्कलन तथा भण्डारणले यसको सम्भावित दुरुपयोग वा शोषणको बारेमा चिन्ता बढाउँछ भने डिजिटल युगमा गोपनीयता अधिकारको उल्लङ्घनलाई अझ बढाउँछ । यस्तो व्यापक निगरानीले अनलाइन सञ्चारमाथिको विश्वासलाई कमजोर बनाउँछ र व्यक्तिहरूको गोपनीयताको भावनालाई कमजोर बनाउँछ, जसले स्व-प्रतिबन्ध (सेल्फ सेन्सरसिप) तथा अभिव्यक्ति स्वतन्त्रतामा दीर्घकालीन प्रभावहरू निम्त्याउँछ । गोपनीयता अधिकारको संरक्षण गर्न पर्याप्त सुरक्षा उपायहरू बिना, राज्य निगरानीको विस्तारले डिजिटल क्षेत्रमा व्यक्तिहरूको स्वायत्तता तथा मर्यादालाई कमजोर बनाउने जोखिम रहन्छ ।

[३] एनआइजीमा ह्याकिंग र जासुसी हुन सक्ने खतरा रहन्छ किनभने सबै इन्टरनेट एउटै चेकपोइन्टबाट जान्छ, यदि गलत व्यक्तिहरुले एनआइजीमा अनाधिकृत पहुँच प्राप्त गर्यो भने, यसले नेपालको सम्पूर्ण इन्टरनेट ट्राफिक हेर्न र निगरानी गर्न सक्षम हुनेछ ।

मुख्य सिफारिसहरु

- अभिव्यक्ति स्वतन्त्रता र गोपनीयताको अधिकारमा अनुचित खतरा निम्त्याउने भएका कारण राष्ट्रिय इन्टरनेट गेटवेको कार्यान्वयन नगर्ने, र
- लागू गरिएका साइबर सुरक्षा उपायहरूले मानवअधिकारको संरक्षणलाई प्राथमिकता दिई अन्तर्राष्ट्रिय मापदण्डहरूको पालना गरेको सुनिश्चित गर्ने ।

२ अनलाइन अभिव्यक्ति स्वतन्त्रता तथा सामग्री प्रकाशनमा गम्भीर प्रतिबन्धहरु

नीतिले यस बारेमा के व्यवस्था गरेको छ ?

नीतिमा अनलाइन अभिव्यक्ति स्वतन्त्रता तथा सामग्री प्रकाशनमा गम्भीर प्रतिबन्धहरू लगाउने निम्न व्यवस्थाहरु रहेका छन्:

- दफा ११.६४: यस दफाको उद्देश्य इन्टरनेट तथा सामाजिक सञ्जालमा "झूटा सूचना" को प्रचारप्रसारलाई नियन्त्रण गर्न कानून बनाई त्यस्ता प्रसारलाई निषेध गर्ने हो ।
- दफा ११.६७: यस दफाले "घृणा वा द्वेष फैलाउने", "साइबर बुलिङ्ग" वा "सामाजिक सद्भावमा खलल पुर्‍याउने" सामग्री लगायत विभिन्न वर्गका डिजिटल सामग्रीहरूलाई निषेध गर्छ ।

मानव अधिकारसम्बन्धी खतराहरु के के छन् ?

अभिव्यक्ति स्वतन्त्रतामा खतरा: यी प्रतिबन्धहरूले सेन्सरसिपको जोखिम निम्त्याउनुका साथै अन्तर्राष्ट्रिय कानून तथा नेपाली संविधानले प्रत्याभूत गरेको अभिव्यक्ति स्वतन्त्रतालाई खतरामा पार्छ । "झूटा सूचना" तथा अन्य अस्पष्ट रूपमा परिभाषित सामग्रीको प्रचारप्रसारलाई निषेध गर्नाले स्वतन्त्र मिडियालाई निरुत्साहित गर्न सक्छ, सार्वजनिक बहसलाई कमजोर बनाउन सक्छ, सरकारी जवाफदेहितालाई कमजोर बनाउँछ, र सुसूचित निर्णयको लागि आवश्यक जानकारीको उपलब्धतामा बाधा पुर्‍याउँछ, जसले लोकतन्त्रलाई नै कमजोर बनाउँछ ।

मुख्य सिफारिसहरु

- कानून तथा नीति नियमहरूमा नीतिको दफा ११.६४ र ११.६७ जस्तो अनलाइन अभिव्यक्ति स्वतन्त्रता तथा सामग्री प्रकाशनमाथि अस्पष्ट तथा व्यापक प्रतिबन्धहरू समावेश नगरिएको सुनिश्चित गर्ने,
- नयाँ तथा पूर्ण निषेध गर्ने प्रावधानहरू भन्दा गाली बेइज्जती वा हिंसालाई दुरुत्साहन जस्ता निश्चित किसिमका कसुर र सजायसम्बन्धी विद्यमान कानूनी प्रावधानहरुको प्रयोग गर्ने; मिथ्या सूचना (डिस्इनफोरमेसन) सम्बन्धी नियोजित अभियानहरुलाई रोक्न स्पष्ट कानून निर्माण गर्ने,
- आम नागरिकलाई मिथ्या सूचना (डिस्इन्फोरमेसन) पहिचान तथा सम्बोधन गर्न, डिजिटल साक्षरता प्रवर्धन गर्न, र जिम्मेवार अनलाइन व्यवहारलाई अभिवृद्धि गर्न सचेतना कार्यक्रमहरू लागू गर्ने ।

३ अनलाइन अभिव्यक्ति र गतिविधिहरूको नियमित अनुगमन

नीतिले यस बारेमा के व्यवस्था गरेको छ ?

यस नीति (दफा १०.८)ले साइबर सुरक्षाका लागि अनलाइन स्पेसको “नियमित अनुगमन”को व्यवस्था गरेको छ । विशेष गरी, यस नीतिले निगरानीमार्फत सुरक्षित साइबर स्पेस निर्माण गर्ने लक्ष्य राखेको छ ।

मानव अधिकारसम्बन्धी खतराहरु के के छन् ?

गोपनीयता अधिकार र निगरानीको लागि जोखिम: नीतिको यस प्रावधानको प्रयोग गरी अनलाइन अभिव्यक्ति तथा गतिविधिहरूको व्यापक, व्यवस्थित र निरन्तर निगरानी गर्न सकिन्छ । यस प्रावधानको उद्देश्य साइबर सुरक्षा बढाउने तथा अनलाइन सुरक्षा सुनिश्चित गर्ने भए पनि यसले व्यक्तिको गोपनीयता तथा अभिव्यक्ति स्वतन्त्रताको उल्लङ्घन हुने गरी हस्तक्षेपकारी निगरानी हुन सक्ने चिन्ता बढाउँछ । यस प्रावधानले अनलाइन गतिविधिहरू व्यापक रूपमा अनुगमन गर्न सरकारलाई सक्षम बनाउँछ, जसले गर्दा व्यक्तिहरूको निजी र सुरक्षित रूपमा सञ्चार गर्ने क्षमतालाई कमजोर बनाउँछ । यस्तो निगरानीमाथि उचित सीमा नहुने हो भने यसको दुरुपयोग भई आलोचनात्मक तथा असहमत आवाज दबाउन वा विशिष्ट समूहहरूलाई लक्षित गर्न दुरुपयोग हुन सक्छ ।

मुख्य सिफारिसहरु

- कुनै पनि अनुगमन गतिविधिहरू असाधारण परिस्थितिहरूमा स्वतन्त्र न्यायिक निकायको कडा निगरानीमा मात्र सञ्चालन गरिएको सुनिश्चित गर्ने,
- अनुगमन शक्तिको दुरुपयोग रोक्न तथा व्यक्तिको गोपनीयता अधिकारको संरक्षण गर्न सुरक्षा उपायहरू लागू गर्ने,
- अनुचित निगरानी रोक्नको लागि अनुगमन गतिविधिहरूको क्षेत्र तथा अवधि स्पष्ट हुने गरी निर्देशिकाहरु बनाउने,
- सार्वजनिक र सान्दर्भिक निगरानी निकाय (जस्तै स्वतन्त्र न्यायिक निकाय)समक्ष अनुगमन गतिविधिहरुको प्रकृति तथा क्षेत्रको बारेमा नियमित जानकारी दिने लगायत अनुगमन प्रक्रियामा पारदर्शिता र जवाफदेहिता प्रवर्द्धन गर्ने,
- मानव अधिकार र सुरक्षा सरोकारहरूबीच सन्तुलनमा राख्ने साइबर सुरक्षा उपायहरूको लागि बहृत् संरचना निर्माण गर्न नागरिक समाज सङ्गठनहरू तथा मानव अधिकार विशेषज्ञहरूसँग सहकार्य गर्ने ।

निष्कर्ष: आगामी बाटो

प्रभावकारी साइबर सुरक्षा संरचनाको लागि सशक्त मानव अधिकार संरक्षण एक बलियो घटक हो। राष्ट्रिय साइबर सुरक्षा नीति २०८० ले नेपालमा साइबर सुरक्षाका लागि राम्रो खाका तयार पारेको छ। यद्यपि, नेपालमा आम नागरिकहरूले सुरक्षित र स्वतन्त्र इन्टरनेटको उपयोग गर्न सकुन् भन्ने सुनिश्चित गर्न यस पत्रमा उल्लेख गरिएका सरोकार तथा चासोहरुलाई भावी कानून तथा नीति नियमहरूले सम्बोधन गर्नै पर्छ। डिआरएन तथा आइसिएनएल सम्बन्धित सरोकारवालाहरूसँग यी सरोकार, चासो तथा विषयवस्तुहरुमाथि थप सहकार्य गर्न सधैँ तत्पर रहेको 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 रहँदै 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।

इन्टरनेशनल सेन्टर नट फर प्रोफिट ल (ICNL) विश्वभरका देशहरूमा नागरिक समाज सङ्गठनहरूका लागि उपयुक्त कानून र नियामक प्रणालीहरूको विकासमा प्राविधिक सहयोग, अनुसन्धान र शिक्षा प्रदान गर्ने अन्तर्राष्ट्रिय संस्था हो। ICNL ले १०० भन्दा बढी देशहरूमा नागरिक समाज, सरकार र नीति विशेषज्ञहरूलाई सहयोग प्रदान गरेको छ। अनलाइन र अफलाइनमा अभिव्यक्ति, सभा, सम्मेलनको स्वतन्त्रता र गोपनीयताको अधिकारको प्रवर्द्धन र संरक्षण गर्नका लागि ICNL ले अन्तर्राष्ट्रिय र क्षेत्रीय संस्थाहरू, निजी संस्थाहरु र स्थानीय सहकर्मीहरूसँग सहकार्य गरेको छ। ICNL को कामको बारेमा थप जानकारीको लागि, कृपया www.icnl.org मा जानुहोस्।