नेपालमा साइबर कसूर सम्बन्धी कानूनको प्रभाव मूल्यांकन

(अनुसन्धानमूलक अध्ययन प्रतिवेदन, २०८१)

प्रकाशक
महान्यायाधिवक्ताको कार्यालय
रामशाहपथ, काठमाडौं

नेपालमा साइबर कसूर सम्बन्धी कानूनको प्रभाव मूल्यांकन

(अनुसन्धानमूलक अध्ययन प्रतिवेदन, २०८१)

अध्ययन कार्यदल

नायब महान्यायाधिवक्ता डा. टेकबहादुर घिमिरे	अनुगमनकर्ता
नायब महान्यायाधिवक्ता श्री खेमराज ज्ञबाली	संयोजक
सहन्यायाधिवक्ता श्री गोबिन्द खनाल	सदस्य
उपन्यायाधिवक्ता श्री पोषराज खनाल	सदस्य
उपन्यायाधिवक्ता श्री पुष्पराज बास्तोला	सदस्य
उप-सचिव श्री राजकुमार महर्जन	सदस्य
प्रहरी उपरिक्षक श्री दिपकराज अबस्थी	सदस्य
सहायक न्यायाधिवक्ता श्री शुभाष भट्टराई	सदस्य
सहायक न्यायाधिवक्ता श्री सुस्मिता पौडेल	सदस्य
सहायक न्यायाधिवक्ता श्री उमंग निरौला	सदस्य-सचिव

प्रकाशनः **महान्यायाधिवक्ताको कार्यालय, नेपाल**

प्रकाशन मितिः २०८१ असार

प्रकाशन संख्याः १००० (एक हजार) प्रति

अध्ययन प्रतिवेदन तयारीको सन्दर्भमा

डिजिटल युगको तीव्र प्रगतिसँगै साइबर अपराधको संख्या र जटिलता वृद्धि भएको छ, जसले समाजको विभिन्न तहमा गम्भीर प्रभाव पारिरहेको छ । साइबर अपराधका विभिन्न प्रकारका जस्तै, डेटा चोरी, फिसिंग, मालवेयर आक्रमण, र अनधिकृत पहुँचले व्यक्तिगत गोपनीयता र राष्ट्रिय सुरक्षामा जोखिम उत्पन्न गरेको छ । यस परिप्रेक्ष्यमा, साइबर अपराधको प्रभावकारी अनुसन्धान र अभियोजन गर्नका लागि समस्या र चुनौतीहरूको विश्लेषण गर्नु अत्यन्त आवश्यक छ । नेपालमा साइबर अपराधको अनुसन्धान र अभियोजनमा देखा परेका समस्याहरू र चुनौतीहरू विश्लेषण गर्दै प्रस्तुत प्रतिवेदनले अत्यन्त महत्वपूर्ण बुँदाहरूलाई उजागर गरेको छ ।

साइबर अपराधको अनुसन्धानमा प्रमुख समस्याहरूमध्ये एक महत्वपूर्ण समस्या भनेको प्रविधिक दक्षताको कमी हो । अनुसन्धान गर्दा प्रयोग हुने प्राविधिक उपकरण र उपायहरूको अभावले गर्दा अपराधको स्रोत पत्ता लगाउन कठिनाइ हुन्छ । साइबर अपराधको प्रवृत्तिहरू समय समयमा परिवर्तन भइरहेका छन्, जसले गर्दा पुराना उपकरण र विधिहरूले नयाँ प्रकारका अपराधहरूलाई समेट्न सक्दैनन् । यसको परिणामस्वरूप, अपराधीहरूको पहिचान र नियन्त्रणमा चुनौतीहरू देखिन्छन् । अर्को प्रमुख समस्या भनेको कानूनी संरचनामा रहेका खोटहरू हुन् । नेपालमा साइबर अपराधसँग सम्बन्धित कानूनी प्रावधानहरू प्रायः पुराना छन् र नयाँ प्रविधिहरूसँग मेल खाँदैनन् । यसका कारण, साइबर अपराधका दोषीलाई न्यायको कठघरामा ल्याउन कानूनी प्रक्रियामा अस्पष्टता र कठिनाइ उत्पन्न हुन्छ । कानूनी व्यवस्थाको सुधार गर्न आवश्यक छ ताकि नयाँ प्रविधि र अपराधीहरूको रणनीतिहरूसँग मेल खाने कानूनी प्रावधानहरू लागू गर्न सकियोस् ।

साइबर अपराधको अनुसन्धान र अभियोजनमा देखा परेका अन्य चुनौतीहरूमा डेटा संरक्षण र गोपनीयताको मुद्दा पनि समावेश छ । डिजिटल प्लेटफर्ममा डेटा प्रवाह र भण्डारणको मात्रा अत्यधिक छ, जसले गर्दा व्यक्तिगत र संवेदनशील सूचनाको संरक्षणमा समस्या आउन सक्छ । यस सन्दर्भमा, डेटा सुरक्षा र गोपनीयता सुनिश्चित गर्न प्रभावकारी विधिहरू लागू गर्नुपर्ने आवश्यकता छ । साइबर अपराधको प्रभावकारी अनुसन्धान र अभियोजनका लागि प्राविधिक दक्षता बढाउनका लागि नियमित प्रशिक्षण कार्यक्रमहरू सञ्चालन गर्नुपर्छ । यसका साथै, साइबर अपराधसँग सम्बन्धित कानूनी ढाँचा र प्रक्रियाहरूलाई अद्यावधिक गर्न नयाँ नीतिहरू र निर्देशिकाहरू निर्माण गर्नुपर्ने आवश्यकता छ । यस अध्ययनमा साइबर अपराधका मुद्दामा संलग्न अधिकृतहरूको क्षमता अभिवृद्धि गर्न र प्रविधिक दक्षता बढाउनका लागि महत्वपूर्ण सुझावहरू प्रस्तुत गरिएको छ ।

अनुसन्धान र अभियोजनका सन्दर्भमा सुधारका लागि विभिन्न उपायहरू अपनाउन सुझाव दिइएको छ । यस्ता उपायहरूमा डेटा सुरक्षा र गोपनीयता सम्बन्धी कानूनी प्रावधानहरूको सुदृढीकरण, साइबर अपराधसँग सम्बन्धित विशेष प्रशिक्षण कार्यक्रमहरूको सञ्चालन, र नवीनतम प्रविधिको समावेशीकरण समावेश छन् । यसले गर्दा, साइबर अपराधका मुद्दामा बढी प्रभावकारी र न्यायोचित निर्णयहरू गर्न सकिन्छ ।

नेपालमा साइबर अपराधको जोखिम र त्यसको नियन्त्रणमा सुधारका लागि एकीकृत प्रयासको आवश्यकता छ । कानूनी ढाँचा, प्राविधिक दक्षता, र संस्थागत समन्वयका आधारमा उपयुक्त सुधारको कार्यान्वयन गरेर, साइबर अपराधको प्रभावकारी अनुसन्धान र अभियोजनलाई सुनिश्चित गर्न सकिन्छ । यस अध्ययनले यस दिशामा महत्वपूर्ण जानकारी र सुझावहरू प्रस्तुत गर्दै, सुधारका लागि मार्गदर्शन पुर्याउँछ ।

साइबर अपराधको वृद्धि र यसको जटिलता बृद्धिसँगै, प्रभावकारी कदम चाल्न र समस्याहरूको समाधान गर्नका लागि समन्वय र सुधारमा ध्यान दिन अत्यन्त महत्त्वपूर्ण छ। यस अध्ययनले नेपालमा साइबर अपराधको अनुसन्धान र अभियोजनमा रहेका समस्याहरू र चुनौतीहरूको सन्दर्भमा आवश्यक सुधारका उपायहरू प्रदान गर्दै, भविष्यमा साइबर अपराधको नियन्त्रण र न्यायको प्रभावकारिता सुनिश्चित गर्न योगदान पुर्याउँछ। यसले सरकारी निकायहरू, कानूनी पेशाकर्मीहरू, र साइबर सुरक्षा विशेषज्ञहरूलाई साइबर अपराधको प्रभावकारी नियन्त्रणको दिशा निर्देशित गर्दै, डिजिटल सुरक्षा र कानूनी सुधारको नयाँ मार्ग प्रशस्त गर्छ।

यो कार्यपत्र तयार गर्न कार्यदलका सबै सदस्यहरूको अथक परिश्रम, समर्पण, र सामूहिक प्रयासको महत्त्वपूर्ण योगदान रहेको छ। साइबर अपराधको अनुसन्धान र अभियोजनका विविध पक्षहरूको विश्लेषण र समस्याहरूको पहिचानमा उहाँहरूका अनुभव, ज्ञान, र प्राविधिक दक्षता अत्यन्तै महत्त्वपूर्ण साबित भएका छन्। प्रतिवेदनमा भएका त्रुटि कमजोरीका लागि क्षमा याचना गर्दछौँ। नायब महान्यायाधिवक्ता डा. टेकबहादुर घिमिरेको अनुगमनमा, संयोजक नायब महान्यायाधिवक्ता श्री खेमराज ज्ञवालीको नेतृत्वमा, सहन्यायाधिवक्ता गोविन्द खनाल, उपन्यायाधिवक्ता पुष्पराज बाँस्तोला, पोषराज खनाल, सहायक न्यायाधिवक्ता सुस्मिता पौडेल, शुभाष भट्टराई, उमंग निरौला साथै काठमाण्डौ स्कुल अफ ल भक्तपुरबाट खटिनु भएका ईन्टरनहरु कविता भुसाल र रज्जु रुषा सिग्देल लगायत अन्य सम्पूर्ण सदस्यहरूको सामूहिक सहयोगले गर्दा यो अध्ययन सफलतापूर्वक सम्पन्न हुन सकेको हो। साइबर अपराधको अनुसन्धान र अभियोजनको क्षेत्रमा देखिएका चुनौतीहरूको समाधान गर्न कार्यदलले प्रस्तुत गरेका सुझावहरू भविष्यमा यस क्षेत्रको सुधार र सुदृढीकरणका लागि महत्वपूर्ण हुनेछन्।

अध्ययन कार्यदल

असार, २०८१

विषय-सूची

परिच्छेद एक

प्रारम्भिक

१.१. अध्ययनको पृष्ठभुमि (Introduction of Study)

सूचनाको क्षेत्रमा भएको क्रान्तिले मानव जीवनलाई सहज, सरल र सुखद तुल्याएको छ। अर्को तर्फ यसले विश्वव्यापी रूपमा समस्या र चुनौती पनि थपिदिएको छ। वर्तमान समयमा सूचना प्रविधिमा भएको बढ्दो विकास संगै अपराधिक क्रियाकलापहरूमा प्रविधिको दुरूपयोग बढ्नुको साथै कसूरका स्वरूपमा नयाँ-नयाँ परिवर्तनहरू देखा परेको छ। कसूरको शैलीमा परिवर्तन ल्याएको छ। पछिल्लो समयमा सूचना प्रविधिको दुरूपयोग गरी हुने साइबर कसूर बढ्दै गएको छ। वस्तुत: साइबर कसूरले त्यस्ता कसूर वा कानुनद्वारा वर्जित क्रियाकलापलाई जनाउँछ जसमा कम्प्युटरजन्य प्रविधि र इन्टरनेट प्रणाली सन्निहित हुन्छ। कम्प्युटर प्रविधि र सोमा आधारित इन्टरनेट संजालको दुरूपयोग गरी आफूले अनुचित फाइदा लिने र अर्को पक्षलाई भौतिक वा आर्थिक नोक्सानी पुऱ्याउने, हैरानी दिने, प्रतिष्ठामा गैरकानुनी आघात पुऱ्याउने, सामुदायिक तनाव बढाउने एवं सार्वजनिक नैतिकतामा खलल पार्ने कुराहरूलाई विभिन्न मुलुकहरूले साइबर कसूरको रूपमा परिभाषित गरी सो अनुरूपको कानूनी व्यवस्था समेत गरेको पाइन्छ। यस सन्दर्भमा नेपालमा विद्युतीय कारोबारलाई निर्देशन, एवं नियमन गर्ने अग्रणी कानूनको रूपमा विद्युतीय (इलेक्ट्रोनिक) कारोबार सम्बन्धी ऐन, २०६३ कार्यान्वयनमा रहेको छ। हाम्रो सन्दर्भमा यो ऐन विशेष कानूनको रूपमा कार्यान्वयनमा आएको हो।

साइवर कसूरको प्रकृतिलाई हेर्दा यसमा संलग्न व्यक्तिहरूले अति विज्ञता र सावधानीका साथ आपराधिक गतिविधिहरू सञ्चालन गर्ने गर्छन्। सूचना र प्रविधिको विकास सँगै विश्वब्यापीकरणको प्रभाव र असरले समेत साइवर कसूरको विकास र विस्तारमा थप सहयोग पुगेको छ। कुनै एक ठाउँबाट गरिने आपराधीक गतिवीधीले सम्पूर्ण विश्वलाई नै असर पुऱ्याउदछ। यस अर्थमा साइवर कसूर अन्तरदेशीय कसूरको रूपमा पनि विकसित हुदै गएकाले यो विश्वव्यापी चुनौतीको विषय समेत बनेको छ। विश्वमा द्रुतरूपमा भएको इन्टरनेटको विकासले ल्याएको सुविधाहरूको प्रयोग गरी सञ्चालनमा आएका सामाजिक सञ्जालको माध्यमबाट साइवर कसूर बढ्दै गएको कुरालाई नेपालले मात्र होइन विश्वका सबै राष्ट्रले स्वीकार गरी यसको नियन्त्रणका लागि समन्वयात्मक प्रयास गरेको अवस्था रहेको छ।

साइवर कसूरको अवधारणाले फौजदारी विधीशास्त्रमा प्रवेश पाएको धेरै लामो समय भएको भने छैन। पछिल्लो समयमा सूचना प्रविधीको बढ्दो विकास र प्रयोगसँगै विद्युतीय प्रविधिलाई दुरूपयोग गरी आर्थिक लाभ लिने, राष्ट्र प्रमुख तथा अन्य व्यक्तिको चारित्रिक हत्या गर्ने, कम्प्युटरबाट व्यक्तिगत देखि संस्थागतसम्मका गोप्य सूचनाहरू सार्वजनिक गर्ने, इन्टरनेटको माध्यमबाट लाखौं रूपैयां ठगि गर्ने, वेबसाइटहरू बिगार्ने, नक्कली एटीएम कार्डबाट पैसा झिक्ने जस्ता लगायतका आपराधीक गतिविधि हुने गरेको प्रवृत्ति देखा परेको देखिन्छ। खास गरी सूचना प्रविधीको प्रयोगको क्रममा आपराधिक गतिविधी हुन थाले पछी यस सम्बन्धी अवधारणालाई फौजदारी विधीशास्त्रमा चर्चा र छलफल अधि बढाइएको हो। साइवर कसूर जटिल र परम्परागत कसूर भन्दा भिन्न प्रकृतिको कसूर भएको हुँदा यसको अनुसन्धान र अभियोजनको क्रममा विशेष सीप, दक्षता, शैली, पद्धतिको अनुसरण अपेक्षित रहन्छ। उपरोक्त परिप्रेक्ष्यमा नेपालमा साइबर कसूरको अनुसन्धान र अभियोजनमा देखा परेका समस्या तथा चुनौतीको अध्ययन गरी प्रस्तुत कार्यपत्र तयार गरिएको छ।

१.२. समस्याको कथन (Statement of the Problem)

वर्तमान समयमा सूचना प्रविधीको प्रयोग गरी गम्भीर घटनाहरू हुने गरेको पाइन्छ । जसले गर्दा साइबर कसूरको सन्दर्भमा थप चुनौती समेत थपिदिएको छ । तथापि, अनुसन्धानकर्ता प्रहरी, अभियोजनकर्ता सरकारी वकिल, मुद्दा छिन्ने न्यायाधीश लगायतका सरोकारवालाहरूमा विधूतीय कारोबार सम्बन्धी कसुरको अवधारणात्मक र प्रयोगात्मक बुझाईको कमी नै रहेको देखिएको छ । तुलनात्मक रूपमा नयाँ कानुन रहेको, प्राविधिक विषय सन्निहित रहेको तथा यस विषयमा सरोकारवालाहरूमा योजनाबद्ध प्रशिक्षणसमेतको अभाब रहेको हुँदा विद्युतीय कारोबार सम्बन्धी कसूरको बुझाइमा कमी रहेको देखिन्छ । यसकारण, सैद्धान्तिक ज्ञान र व्यावहारिक तालिमको अभावमा अनुसन्धानका क्रममा सार्थक निर्देशन तथा अभियोजनको पाटोमा समेत अपेक्षित प्रभाबकारीता कायम हुन सकेको छैन । विद्युतीय कसूर अन्तर्गतका मुद्दामा न्यायिक दृष्टिकोणको चर्चा गर्नुपर्दा अधिकांश मुद्दामा वादी नेपाल सरकार असफल हुने पाइएको छ । साइबर कसूरको सन्दर्भमा विकसित सबै विषयलाई विद्यमान विद्युतीय कारोबार ऐनमा समावेश हुन सकेको अवस्था पनि छैन । अभिव्यक्ति स्वतन्त्रताको प्रयोग गर्दा अनावश्यक रूपमा आकर्षित गराइएको गुनासाहरू बढ्दै गएका छन् ।

उपरोक्त सन्दर्भमा प्रस्तुत कार्यपत्रमा मुलतः देहायका समस्याहरूमा अध्ययन केन्द्रित गरिएको छ ।

(१) साइबर कसूरको अनुसन्धान र अभियोजन सम्बन्धमा के कस्ता समस्या तथा चुनौतीहरूको विद्यमानता रहेको छ ?

(२) साइबर कसूरको अनुसन्धान र अभियोजनमा देखिएका समस्या तथा चुनौतीको सम्वोधन गर्न के कस्ता उपायहरू अवलम्वन गर्न उपयुक्त हुन्छ ?

१.३ अध्ययनको उद्देश्य (Objectives of the Study)

प्रस्तुत अध्ययनको उद्देश्य निम्न बमोजिम रहेका छन् ।

(१) साइबर कसूर सम्बन्धी कानूनको समग्र स्थितिका सम्बन्धमा जानकारी प्राप्त गर्ने,

(२) साइबर कसूर सम्बन्धी अवधारणात्मक पक्षको बारेमा जानकारी प्रदान गर्नु,

(३) साइबर कसूर सम्बन्धी कानूनको प्रवृत्ति, कसूरको तरिकाको विश्लेषण गर्नु,

(४) साइबर कसूरको अनुसन्धान र अभियोजन सम्बन्धमा रहेका समस्या तथा चुनौतीहरू पहिचान गर्नु,

(५) साइबर कसूर सम्बन्धी कानूनका विभिन्न प्रवृत्ति र प्रकृतिका सम्वन्धमा सर्वोच्च अदालतबाट प्रतिपादित सिद्धान्तको सर्वेक्षण र विश्लेषण गर्ने

(६) पहिचान भएका समस्या तथा चुनौतीहरूको सामना गर्नको लागि अवलम्बन गर्नु पर्ने उपायहरू सिफारिस गर्नु ।

१.४ अध्ययनको सिमा (Limitation of the Study)

प्रस्तुत अध्ययन साइबर कसूर सम्बन्धी कानूनको प्रवृत्ति विश्लेषण तथा कानूनको प्रभाव मूल्याङ्कन सम्बन्धमा भएका कानूनी व्यवस्थाको कार्यान्वयनको प्रभावकारिता मूल्याङ्कनमा केन्द्रित रहेको छ । साइबर कसूर सम्बन्धी कानूनको

अनुसन्धान तथा अभियोजनमा संलग्न अधिकृतहरुबाट संकलन गरिएका प्रश्नावली, विज्ञहरुको अन्तरवार्ताको विश्लेषण तथा छनोट गरिएका अभियोगपत्रहरुको अध्ययन, सर्वोच्च अदालतबाट प्रतिपादित सिद्दान्तहरुको कार्यान्वयन तथा साइबर कसूर सम्बन्धी कानूनको विद्यमान कानूनमा सुधारका क्षेत्रहरुको पहिचानमा सीमित रही अध्ययन गरिएको थियो। यस अध्ययन नेपालमा साइबर कसूरको अनुसन्धान र अभियोजन सम्बन्धमा रहेका समस्या तथा चुनौतीहरूको सन्दर्भमा मात्र केन्द्रित रहनेछ। प्रस्तुत अध्ययनको माध्यमबाट नेपालमा साइबर कसूरको अनुसन्धान तथा अभियोजनमा रहेका समस्या तथा चूनौतीको पहिचान गरी सो को सम्बोधनको लागि आवश्यक पर्ने उपायको खोजी गरिनेछ।

१.५ अध्ययन विधि (Methodology of the Study)

यस अध्ययनमा मिश्रित बिधि (Mixed Approach) प्रयोग गरिएको छ। संविधान, नीति, ऐन, नियम, पुस्तक, पत्रिका, जर्नल, म्यागेजिन, सरकारी कार्यालयमा रहेका अभिलेख, इन्टरनेट, वेवसाइट, प्रकासित तथा अप्रकासित सोधमुलक लेख जस्ता श्रोतबाट अध्ययनको विषयसँग सम्बन्धीत तथ्य, सूचना तथा तथ्यांकहरू संकलन गरिएका छन्। यसका लागि साइबर कसूर सम्बन्धी कानूनहरुको अभियोगपत्र तथा फैसलाको अध्ययन गरी निश्चित सुचकहरूमा आधारित रही संख्यात्मक बिश्लेषण बिधि (Quantitative Approach) प्रयोग गरिनेछ भने साइबर कसूर सम्बन्धी कानूनहरूको ऐन नियम, निर्देशिका तथा अन्य कानूनी व्यवस्थाहरुको अध्ययन/सर्वेक्षण, सर्वोच्च अदालतबाट साइबर कसूर सम्बन्धी मुद्दामा प्रतिपादन भएका प्रकाशित तथा अप्रकाशित खास गरी कसूर अनुसन्धान तथा अभियोजनका सम्बन्धमा भएका टिप्पणी, निर्देशनात्मक आदेशहरुको संकलन गरी कसूर कायमको स्थिति, कसूरहरूको अनुसन्धान र अभियोजनका सम्बन्धमा भएका आदेश, निर्देशन, टिप्पणी एवं मार्गदर्शनको सर्वेक्षण र त्यसको कार्यान्वयनको अवस्थाको अध्ययन तथा साइबर कसूर सम्बन्धी कानूनमा विभिन्न निकायबाट गरिएका मूख्य अध्ययन सामग्रीको समीक्षामा आधारित भइ गुणात्मक बिश्लेषण बिधि (Qualitative Approach) को प्रयोग गरिनेछ।

प्रस्तुत अध्ययनमा देहायका विधिहरु अवलम्वन गरिएको छः

- **अध्ययन सर्वेक्षणः** साइबर कसूर सम्बन्धी ऐन नियम, निर्देशिका तथा अन्य कानूनी व्यवस्थाहरुको अध्ययन/सर्वेक्षण, समयानुकूल सुधारका क्षेत्रहरु पहिचान गरिएको छ।

- **प्रश्नावलीः** साइबर कसूर सम्बन्धी कानूनको कानूनी व्यवस्था तथा कार्यान्वयनमा गर्नुपर्ने सुधारका सम्बन्धमा प्रश्नावली तयार गरी साइबर कसूर सम्बन्धी मुद्दाको मिसिल अध्ययन गरी निश्चित Indicator को आधारमा सूचनाको तालिकीकरण र विश्लेषण गरिएको छ।

- **अभियोगपत्र अध्ययनः** महान्यायाधिवक्ताको कार्यालयको आ.व. २०७९/०८० को वार्षिक प्रतिबेदनमा साइबर कसूर सम्बन्धि कुल २५२ मुद्दाहरूको फछ्र्यौट भएकोमा समग्र मुद्दाको समानुपातिक प्रतिनिधित्व हुनेगरी Simple Ramdom Sampling बिधि मार्फत २०% ले हुन आउने जम्मा ५० वटा मुद्दाका मिसिलका अभियोगपत्र, पुनरावेदनपत्र लगायत आवश्यक कागजात विद्युतीय माध्यमबाट प्राप्त गरी अध्ययन, विश्लेषण गरिएको छ।

- **सर्वोच्च अदालतबाट भएका आदेशको अध्ययनः** सर्वोच्च अदालतबाट साइबर कसूर सम्बन्धी मुद्दामा प्रतिपादन भएका प्रकाशित तथा अप्रकाशित खास गरी साइवर कसूर अनुसन्धान तथा अभियोजनका

सम्बन्धमा भएका टिप्पणी, निर्देशनात्मक आदेशहरुको संकलन गरी कसूर कायमको स्थिति, कसूर अनुसन्धान र अभियोजनका सम्बन्धमा भएका आदेश, निर्देशन, टिप्पणी एवं मार्गदर्शनको सर्वेक्षण र त्यसको कार्यान्वयनको अवस्थाको अध्ययन र विश्लेषण गरिएको छ।

- **पूर्व अध्ययनको समीक्षाः** साइबर कसूर सम्बन्धी कानूनका विभिन्न निकायबाट गरिएका मूख्य अध्ययन सामग्रीको समीक्षा गरिएको थियो।

१.६ अध्ययनको औचित्य (Rational of Study)

यस अध्ययन नेपालमा साइबर कसूरको अनुसन्धान, अभियोजनमा रहेका समस्या चुनौती तथा सो को सम्वोधनको लागि अवलम्वन गर्नु पर्ने कार्यहरूसँग केन्द्रित रहेको छ। हालसम्म नेपालमा साइबर कसूरको अनुसन्धान, अभियोजनमा रहेका समस्या चुनौती तथा सो को सम्वोधनको लागि अवलम्वन गर्नु पर्ने कार्यहरूको बारेमा वृहत अध्ययन हुन सकेको देखिदैन। यस अध्ययनको माध्यमबाट साइबर कसूरको अनुन्धान र अभियोजनको कार्यमा प्रभावकारीता अभिबृद्धी गर्नमा सहयोग पुग्ने भएको हुँदा प्रस्तुत अध्ययनको औचित्य रहेको छ।

१.७ अध्ययनको रूपरेखा (Organization of the Study)

प्रस्तुत अध्ययनलाई संगतिपूर्ण र व्यवस्थित रूपमा प्रस्तुत गर्न छ वटा परिच्छेदमा विभाजन गरिएको छ। प्रत्येक परिच्छेदलाई निम्न लिखित शिर्षक चयन गरि प्रस्तुत गरिएको छ।

परिच्छेद एकः प्रारम्भिक

परिच्छेद दुईः साइबर कसूरको अवधारणा, विकासक्रम र अन्तराष्ट्रिय नीति, कानून तथा अभ्यास

परिच्छेद तीनः साइबर कसूर सम्बन्धी अध्ययन कार्यको पुनरावलोकन तथा समिक्षा

परिच्छेद चारः साइवर कसूर सम्बन्धमा संवैधानिक, कानूनी, नीतिगत, संस्थागत, पद्धतिगत व्यवस्था

परिच्छेद पाँचः सर्वोच्च अदालतबाट प्रतिपादित नजिर तथा निर्देशनको विश्लेषण

परिच्छेद छः संकलित सूचना/तथ्याङ्क र सोको विश्लेषण

परिच्छेद सातः अध्ययनमा देखिएका समस्या र चुनौतीहरू, सुझाव तथा निष्कर्ष

१.८. कार्यदलको गठन र कार्यादेश

नेपालमा साइबर कसूरको अध्ययन विषयमा अनुसन्धानमूलक अध्ययन गरी अनुसन्धान प्रतिवेदन प्रस्तुत गर्न देहाय बमोजिमको कार्यदल गठन भएको थियो।

पद, नाम	कार्यालय	जिम्मेवारी
नायब महान्यायाधिवक्ता डा.टेकबहादुर घिमिरे	महान्यायाधिवक्ताकोकार्यालय	अनुगमनकर्ता
नायब महान्यायाधिवक्ता श्री खेमराज ज्ञबाली	महान्यायाधिवक्ताको कार्यालय	संयोजक
सहन्यायाधिवक्ता श्री गोबिन्द खनाल	महान्यायाधिवक्ताको कार्यालय	सदस्य
उपन्यायाधिवक्ता श्री पोषराज खनाल	महान्यायाधिवक्ताको कार्यालय	सदस्य
उपन्यायाधिवक्ता श्री पुष्पराज बास्तोला	महान्यायाधिवक्ताको कार्यालय	सदस्य
उप-सचिव श्री राजकुमार महर्जन,	सञ्चार तथा सूचना प्र. मन्त्रालय	सदस्य
प्रहरी उपरिक्षक श्री दिपकराज अबस्थी	साइबर ब्युरो, नेपाल प्रहरी	सदस्य
सहायक न्यायाधिवक्ता श्री शुभाष भट्टराई	महान्यायाधिवक्ताको कार्यालय	सदस्य
सहायक न्यायाधिवक्ता श्री सुस्मिता पौडेल	महान्यायाधिवक्ताको कार्यालय	सदस्य
सहायक न्यायाधिवक्ता श्री उमंग निरौला	महान्यायाधिवक्ताको कार्यालय	सदस्य-सचिव

कार्यदलको कार्यादेश देहाय बमोजिम रहेको थियो:

१. गत आ.व.सम्म साइबर कसूरको क्षेत्राधिकार काठमाण्डौ जिल्ला अदालतमा मात्र रहेकोले उक्त अदालतमा चालु मिसिलका अभियोगपत्र, पुनरावेदनपत्र लगायत आवश्यक कागजात विद्युतीय माध्यमबाट प्राप्त गरी अध्ययन, विश्लेषण गर्ने,

२. अनुसन्धान प्रतिवेदन तयार गर्दा साइबर कसूर सम्बन्धी कानूनको प्रवृत्ति, कसूर गर्दाको तौर तरिकाको विश्लेषण गर्नुका साथै कानून कार्यान्वयनको अवस्था र अनुसन्धान तथा अभियोजनका सन्दर्भमा सुधार गर्नुपर्ने विषय पहिचान गर्ने,

३. अनुसन्धान समूहबाट तयार भएको अनुसन्धान प्रतिवेदनलाई सम्भव भएसम्म सम्बन्धित विज्ञसमेतको सहभागितामा राष्ट्रिय कार्यशाला आयोजना गरी सुझाव लिई अन्तिम रूप दिने र महान्यायाधिवक्ताको कार्यालयको निर्णय बमोजिम प्रतिवेदनको छपाई सम्बन्धी आवश्यक कार्य गर्ने,

४. प्रचलित कानून, नीति, निर्देशिका, पूर्व अध्ययन सामग्री एवं अध्ययन, संकलन गरिएका तथ्य र तथ्याङ्कका आधारमा स्वीकृत ढाँचामा अनुसन्धान प्रतिवेदनको मस्यौदा तयार गर्ने,

५. साइबर कसूर सम्बन्धी कानूनका विभिन्न प्रवृत्ति र प्रकृतिका सम्वन्धमा सर्वोच्च अदालतबाट प्रतिपादित सिद्धान्तको सर्वेक्षण र विश्लेषण गर्ने,

परिच्छेद दुई

साइबर कसूरको अवधारणा, विकासक्रम र अन्तराष्ट्रिय नीति, कानून तथा अभ्यास

२.१ साइबर कसूरको अवधारणा र विकासक्रम (Conceptual Background and Development of Cyber Crime)

२.१.१ साइबर कसूरको अवधारणागत पृष्ठभूमि (Conceptual Background of Cyber Crime)

लोकतान्त्रिक राज्य व्यवस्थाको मापन गर्ने विभिन्न आधारभूत मापदण्डहरू मध्ये विचार तथा अभिव्यक्ति स्वतन्त्रताको प्रत्याभूति पनि एक महत्वपूर्ण मापदण्ड हो। सूचना तथा संचार प्रविधि एवं इन्टरनेटको विकासले व्यक्तिको विचार तथा अभिव्यक्ति स्वतन्त्रताको अभ्यासमा महत्वपूर्ण योगदान पुर्‌याएको छ। साईवरको प्रयोगले भौगोलिक तथा राजनीतिक सीमाबाहिर पुगी समष्टिगत विश्व नै मानव ग्रामको रूपमा निकटतामा परिबर्तित हुन पुगेको छ। त्यसैले, आजको युगलाई सूचना र प्रविधीको युग भन्ने गरिएको छ। अब ज्ञानवान र शक्तिवान व्यक्ति वा मुलुकको मापन सूचना र त्यसको अधिकतम प्रयोगसंग जोडिएकोले एउटा कल्याणकारी राज्यमा इन्टरनेट पहुँचको सुविधा हुनु र पाउनुपर्छ भन्ने विश्वव्यापी मान्यता रहेको छ। इन्टरनेटमा बढ्दै गएको पहुँच, अवसरका अलावा यसले निम्त्याएका समस्या र चुनौती पनि बढ्दै गएका छन्। सूचना प्रविधिको विकाससंगै वढेको इन्टरनेटको प्रयोगले फेसबुक, ट्वीटर, इन्स्टाग्राम, हवाटएप्स, वीच्याट, भाइबर, स्काइप, इमो, म्यासेन्जर जस्ता सामाजिक सञ्जालको प्रयोग व्यापक रूपमा भई रहेको छ। फलस्वरूप विश्वमा साइबर कसूर पनि बढेर गएको छ।

२.१.२ साइबर कसूरको परिचय (Introduction to Cyber Crime)

कुनै पनि किसिमको त्यस्तो गैरकानूनी योजना जसमा दुई वा सोभन्दा बढी इन्टरनेट संजाल जस्तै; चाटरुम, इमेल, मेसेजबोर्ड, वेभसाइट आदि प्रयोग गरेर जालसाजी कार्य वा आर्थिक कारोवारको प्रक्रियामा जालसाजी गरिन्छ साथै, जस अन्तर्गत Spam mails, Virus वा Spyware कम्प्यूटमा पठाउने, कसैलाई इन्टरनेटको माध्यमले हैरानी गर्ने कार्य गरिन्छ; त्यस्तो कार्य Cyber Crime हो।

सामान्य अर्थमा विद्युतीय अपकरणहरूको उपयोग तथा प्रयोग मार्फत गरिने आपराधिक गतिविधिहरू साइबर क्राइम हुन्। यसलाई विश्वव्यापी रूपमै फैलिएको एउटा सङ्गठित कसूरका रूपमा लिने गरिन्छ। सूचना प्रविधि उपयोग मार्फत अनधिकृत पहुँच स्थापित गरी व्यक्तिगत, संस्थागत र सार्वजनिक सुरक्षामा गम्भीर खलल पार्ने विषय साइबर प्राइम हो। कम्प्युटरसँग सम्बन्धित वा विद्युतीय उपकरणहरुलाई माध्यम बनाएर कानुनले निषेध गरेका क्रियाकलापहरू गर्ने कार्यलाई साइबर प्राइम भनिन्छ। साइबर प्राइम कम्प्युटर, नेटवर्क, इमेल, इन्टरनेट सामाजिक सञ्जालको प्रयोग मार्फत गरिने फौजदारी र सङ्गठित कसूर हो। यस प्रकृतिको कसूरमा कुनै किसिमको भौगोलिक वा क्षेत्रगत सिमा नरहने हुँदा यसलाई विश्वव्यापी कसूरमा रूपमा समेत लिन सकिन्छ। साइबर कसूर त्यस्तो प्रकृतिको कसूर हो जसले कम्प्युटर वा विद्युतीय उपकरणलाई माध्यम बनाई वा अर्काको कम्प्युटरमा अनधिकृत पहुँच स्थापित गरी आपराधिक

मानसिकताबाट अरुलाई दुःख दिने वा हानी नोक्सानी पुर्‍याउने एउटा सामाजिक कसूर हो।

इन्टरनेटको प्रयोग गरेर अनलाइनको माध्यमबाट गरिएका कसूरहरू साइबर कसूर हुन्। कम्प्युटर, ल्यापटप, ट्याबलेट, इन्टरनेट जडित टेलिभिजन, स्मार्टफोन आदीको प्रयोग गरी यस्तो कसूर हुने गर्छ। यसकारण कम्प्युटर वा कम्प्यूटर नेटवर्क वा नेटवर्क उपकरण प्रयोग गरी गरिएको आपराधिक गतिविधिलाई साइबर कसूरको रूपमा लिन सकिन्छ। यही सन्दर्भमा विद्वान् Halder & Jaishankar ले गरेको परिभाषा मननीय रहेको छ। उनका अनुसार Cyber Crime is an Offence that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental hurt, or loss, to the victim directly or indirectly, victimization trendy telecommunication networks like Internet".

कम्प्युटर, नेटवर्क, प्रविधि र उपकरणहरूको दुरूपयोग गरी हुने आपराधिक गतिविधी नै साइवर कसूर हो। यस्तो किसिमको कसूर गर्नको लागि कम्प्युटर प्रविधीलाई कसूरको मुख्य हतियारको रूपमा प्रयोग गरिएको हुन्छ। कम्प्यूटर प्रविधि र सोमा आधारित इन्टरनेट सञ्जालको दुरूपयोग गरी आफूले अनुचित फाइदा लिने र अर्को पक्षलाई भौतिक वा आर्थिक नोक्सानी पुर्‍याउने, हैरानी दिने, प्रतिष्ठामा गैरकानूनी आँच पुर्‍याउने, सामुदायिक तनाव बढाउने एवं सार्वजनिक नैतिकतामा खलल पार्ने कसूर नै साइबर कसूर हो। इन्टरनेट, इन्ट्रानेट र एक्स्ट्रानेटसँग सम्बन्धित वेवसाइट तथा इमेल ह्याकिङ, चरित्रहत्या, डाटा चोरी, इन्टरनेटमार्फत व्ल्याकमेलिङ, इन्टरनेट बैंकिङ जालसाजी, अर्काको पहिचान अनधिकृत रूपमा प्रयोग, क्रेडिट कार्ड, अर्काको कम्प्युटर, विद्युतीय उपकरण तथा नेटवर्कमा पुर्‍याउने क्षति, जालसाजी लगायतका आपराधिक गतिविधिहरू साइबर कसूरको रूपमा रहेका छन्।

Dr. Vishwanath Paranjape ले साइबर कसूरलाई व्यक्ति, समाज र राज्य विरूद्ध निम्नानुसार व्याख्या गरेका छन। [१]

व्यक्ति विरूद्ध हुने साइवर कसूर	सम्पत्ति विरूद्ध हुने साइवर कसूर	राज्य तथा समाज विरूद्ध हुने साइवर कसूर
Cyber Stalking	Sale of Illegal Articles	Intrusion of Computer System to extract secret Information
Dissemination Obscene Materials	Inter time Theft	Cyber Terrorism
Unauthorized Control Access over Computer System	Intellectual Property Crime	Distribution of Private Software
Indecent exposure	Unauthorized Access over Computer System	Illegal Human Trafficking Online
Email Spoofing	Denial of Service Attack	Financial Frauds

१ Vishwanath Paranjape (Dr.) (२०१०), Cyber Crimes and Law, India: Central Law Agency, p. २९.

व्यक्ति विरूद्ध हुने साइवर कसूर	सम्पत्ति विरूद्ध हुने साइवर कसूर	राज्य तथा समाज विरूद्ध हुने साइवर कसूर
Pornography	Virus Transmission	Online Gambling
Harassment Via Email	Computer Vandails	Sale of Illegal Articles

२.१.३ साइबर कसूरको स्वरूप (Form of Cyber Crime)

साइबर कसूरको स्वरूपलाई यस प्रकार उल्लेख गर्न सकिन्छ।[२]

१. Hacking: Hacking भनेको सम्बन्धित व्यक्तिको अनुमति बिना उसको कम्प्युटर प्रणालीमा पहुँच पुर्‌याई गरिने कार्य हो।

२. Virus Dissemination: भाइरस एक किसिमको कम्प्युटर प्रोग्राम हो। यसले कम्प्युटर प्रणाली वा फाइलहरूलाई संक्रमित गर्दछ। यसको अन्य कम्प्युटरहरूमा सर्कुलेट हुने प्रवृत्ति हुन्छ। भाइरसले कम्प्युटर अपरेशनमा अवरोध खडा गर्छ र भण्डार गरिएको डाटालाई असर गर्छ।

३. Logic Bombs: यो एक किसिमको Slag Code हो जसलाई कम्प्युटर प्रणालीलाई अवरोध गर्न जानाजानी सफ्टवेयरमा सम्मिलित गरिएको हुन्छ। यो भाइरस होईन। यद्यपि यसले भाइरसको जस्तो कार्य गर्छ।

४. Denial-of-Service Attack: कम्प्युटर प्रणालीको सेवा अवरूद्ध गर्ने कार्यलाई Denial-of-Service attack भनिन्छ।

५. Phishing: यो क्रेडिट कार्ड नम्बरहरू, प्रयोगकर्ताको नाम, पासवर्ड जस्ता गोप्य जानकारी निकाल्ने कार्य हो। यसमा इमेलको प्रयोग गरी Phishing गर्ने गरिन्छ।

६. Email Bombing and Spamming: ईमेल खातामा धेरै संख्यामा ईमेल पठाउने र नेटवर्क स्रोतलाई सेवा गर्न नदिने अवस्थामा पुर्‌याउने कार्य Email bombing and spamming हो।

७. Web Jacking: जालसाजीपूर्वक कसैको वेब साइटलाई नियन्त्रणमा लिइ साइटको सामग्री परिवर्तन गर्ने कार्य Web jacking हो।

८. Cyber Stalking: यो साइवर कसूरको नयाँ रूप हो। यसमा कुनै पनि व्यक्तिको अनलाइन गतिविधिलाई पछ्याई उसको बारेमा जानकारी लिने, सताउने, धम्की दिने आदि कार्य गरिन्छ। यसलाई अनलाइन गोपनीयता विरूद्धको आक्रमणको रूपमा पनि लिन सकिन्छ।

९. Data Diddling: कुनै कम्प्युटर प्रणालीमा प्रवेश गर्नु अघि र प्रवेशको बखत डाटाको अनधिकृत फेरबदल गर्ने कार्य Data Diddling हो।

१०. Identity Theft and Credit Card Fraud: व्यक्तिको पहिचान गरी उसको नाममा रहेका क्रेडिट कार्ड, बैंक खाताहरू आदिमा पहुँच पुर्‌याई सो को प्रयोग गर्ने तथा व्यक्तिको पहिचानलाई अन्य कसूरहरू गर्न प्रयोग गर्ने कार्य Identity Theft and Credit Card Fraud हो।

---

२ https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-१२-types-of-cyber-crime.html (Accessed on February ८, २०२४)

११. Salami Slicing Attack: साइबर-अपराधीहरूले एक पटकमा पैसा वा स्रोतहरू थोरै चोरी गर्ने कार्यलाई Salami Slicing Attack भनिन्छ।

१२. Software Piracy: अनधिकृत रूपमा कम्प्युटर सफ्टवेयरको प्रयोग र वितरण Software Piracy हो।

१३. जालसाजी (Fraud) : कसैलाई कुनै चिठ्ठा परेको वा अवसर प्राप्त भएको वा त्यस्तो चिठ्ठा वा अवसर प्राप्त हुने भनी कुनै कार्य गर्न लगाउने कार्य जालसाजी हो। उदाहरण भनी पठाउने र व्यवस्थापन खर्च भनी रकम माग गर्ने।

१४. गलत कागजात तयार गर्ने (Preparing False Documents) : कम्प्युटरको गलत प्रयोग गरी नक्कली प्रमाणपत्र बनाउने, नक्कली भिषा स्टिकर बनाउने, भिषा सम्बन्धी नक्कली कागजात तयार गर्ने, एकको फोटो स्क्यानिङ्ग गरेर अर्काको नाममा टाँस गर्ने कार्यलाई गलत कागजात तगार गर्ने भनिन्छ।

१५. अश्लीलता (Pornography) : अश्लील चित्र वा भिडियो तयार गरी कसैलाई पठाउने वा यौन प्रस्ताव राख्ने वा सोको लागि रकम माग गर्ने वा पठाउन लगाउने कार्य अश्लिलता हो।

१६. तनाव सिर्जना (Harassment) : कसैलाई बारम्बार Message पठाई तनाव गराउने, प्रेम प्रस्ताव राख्ने र सोको लागि धम्की समेत सिर्जना गर्ने कार्य तनाब सिर्जना हो।

१७. कारोबारको अपचलन गर्ने : विद्युतीय यन्त्र वा प्रणालीको दुरूपयोग गरी कारोबारमा अपचलन गर्ने। जस्तै एटिएम कार्डको पिन नम्बर ह्याक गरेर अरूको रकम निकाल्ने, एउटाको बैंक खाताको रकम अर्कैको नाममा हालिदिने, कुनै टिभी स्टेशनको प्रसारण ब्ल्याक आउट गर्ने, आदि कार्यले कारोबारको अपचलनलाई जनाउँदछ।

२.१.४ साइबर कसूरको प्रकारहरु (Types of Cyber Crime)

१. **ह्याकिङ् वा अनधिकृत पहुँच:** कतिपय इन्टरनेट वा विभिन्न माध्यमबाट ह्याकिङ् वा अनधिकृतरुपको पहुँचबाट पनि साइबर कसूर हुने गरेको छ। सामान्य रुपमा ह्याकिङको अर्थ कुनै कम्प्युटर वा कम्प्युटर प्रणालीमा अनधिकृत पहुँच र नियन्त्रण हो। ह्याकिङ् गर्ने व्यक्तिले कम्प्युटर वा कम्प्युटर प्रणालीमा रहेको कुनै कार्यक्रम, सूचना वा तथ्याङ्कमा उक्त कम्प्युटरको धनी वा जिम्मेवार व्यक्तिको अनुमति वा अख्तियारी नलिइकन पहुँच प्राप्त गर्ने प्रयास गरेर नियन्त्रण स्थापित पनि गर्दछ।

२. **कम्प्युटर भाइरस**: कम्प्युटर भाइरसको प्रयोग गरेर पनि साइबर कसूर हुने गरेको तथ्य हामिले सुन्दै आएका छौँ। कम्प्युटर भाइरस एक किसिमको कम्प्युटर कार्यक्रम वा कोड हो, जसले आफुलाई पुनः उत्पादन गर्दै सम्पर्कमा आउने अन्य उपकरणमा सर्न सक्छ। कम्प्युटरमा रहेका अन्य दस्तावेज, सूचना, तथ्याङ्क र कार्यक्रमलाई नष्ट गर्न वा कम्प्युटरको कार्यलाई असर गर्न सक्छ। अन्ना कोर्निकोभा भाइरस, आइलभयु भाइरस र मेलिसा भाइरस केही नाम चलेका र खतरनाक कम्प्युटर भाइरसहरू हुन् कम्प्युटर भाइरससहित कम्प्युटरलाई असर गर्ने अन्य प्रकारका फाइल वा कार्यक्रमहरलाई "मालवेयर" भनिन्छ। यस्ता कम्प्युटर भाइरसहरु पत्ता लगाउन रोक्न तथा नियन्त्रण गर्न बनाइएका कम्प्युटर कार्यक्रम वा कोडलाई एन्टीभाइरस भन्ने गरिएको छ।

३. **फिसिङ् :** फिसिङ् भनेको जालसाजी गरी व्यक्तिको गोप्य जानकारी जस्तै पासवर्ड वा बैँक कार्ड नम्बर पत्ता लगाउने तरिकाबाट पनि साइबर कसूर हुने गरेको छ। जालसाजी गरी पत्ता लागेका जानकारी पहिचान चोरी वा ठगीका लागि प्रयोग गरिन्छ। जसलाई फिसिङ् पनि भनिन्छ। यसरी फिसिङ् गर्दा प्रायजसो नाम चलेको संस्थाको नाम दुरुपयोग गरी इमेल पठाएर पासवर्ड परिवर्तन गर्न वा अन्य व्यक्तिगत सूचना भर्न लगाइन्छ त्यसरी आएको इमेलमा भएको लिंक अथवा संगै आएको फाइलमा बैंकको खाता नम्बर मागिएको वा पासवर्ड तुरुन्त परिवर्तन

गर्नुपर्ने, वा चिट्ठा परेकोले सो रकम प्राप्त गर्न प्रशासकीय शुल्क तिर्नुपर्ने बताइएको हुन्छ। इमेलका पासवर्ड तुरुन्त परिवर्तन गर्न लिङ्कसहितको इमेल वा कुनै पुरस्कार वा सेवा दाबी गर्न भर्न दिइने फारामहरू वा मागिने पैसाहरू फिसिङका उदाहरणहरु हुन।

४. **डिजिटल चोरी**: कम्प्युटर सफ्टवेयर, गेम वा कोडस चलचित्र वा म्युजिक भिडियोस सङ्गीत वा पुस्तक आदिको गैरकानुनी उत्पादन तथा विक्रि वा वितरण डिजिटल पाइरेसी हो प्रतिलिपि अधिकार भएको व्यक्ति वा संस्था बाहेकको अन्य व्यक्तिले कुनै डिजिटल वस्तु कपी गरी पुनः उत्पादन, विक्री वा वितरण गर्दा त्यो चोरी हुन्छ। यो पनि साइबर कसूर भित्र पर्दछ। अनधिकृतरुपमा चोरी गरिएका त्यस्ता सामग्रीहरू डाउनलोड गरेर आफ्नो उपकरणमा राख्नु वा उपभोग गर्नुपनि कसूर हो नेपालजस्तो विकासोन्मुख देशहरूमा डिजिटल चोरीको समस्या ज्यादा रहेको छ।

५. **इन्कारी आक्रमण**: नेपालमा साइबर कसूरको रुपमा सेवाको इन्कारी आक्रमण पनि हुने गरेको छ। सेवाको इन्कारी आक्रमण नेटवर्क सर्भर विरुद्धको आक्रमण हो जसमा सर्भरले सम्बोधन गर्न नसक्ने गरी ज्यादै ठुलो संख्यामा सेवाको अनुरोध पठाएर र वेबसाइट वा सेवालाई चल्नै नसक्ने बनाइन्छ। यसबाट सो सेवा प्राप्त गर्न चाहने बास्तविक सेवाग्राहीहरूलाई सेवाको इन्कारी हुनजान्छ।

६. **अनलाइन घोटला**: साइबर कसूरकै रुपमा घोटाला वा जालसाजी पनि बढ्दै गएको छ। यो परम्परागत कसूर हो र यदि यस्तो घोटाला वा जालसाजी इन्टरनेट वा कम्प्युटरको प्रयोग गरी गरिन्छ भने त्यसलाई अनलाइन घोटाला वा जालसाजी भनेर चिन्ने गरिन्छ। उदाहरणका लागि विभिन्न अफ्रिकी मुलुकहरूबाट पैसा स्थानान्तरण गर्नु परेकोले सहयोग गर्नुपर्यो भन्दै आउने इमेल वा सोसल मिडियाहरूबाट वा वेबसाइट मार्फत जालसाली सूचनाहरू प्रवाह गरेर गरिने ठगीहरू हुन।

७. **पहिचान चोरी**: पहिचान चोरी पनि साइबर कसूरको अर्को पाटो हो। अर्को व्यक्तिको व्यक्तिगत पहिचान खुल्ने सूचना वा जानकारी प्राप्त गरी उक्त सूचना र जानकारीको आधारमा उक्त व्यक्तिजस्तो बनेर विभिन्न लाभ लिने वा आपराधिक क्रियाकलापमा संलग्न हुनु हो। त्यस्तो व्यक्तिगत पहिचान जानकारी अन्तर्गत उक्त व्यक्तिको नाम वा नागरिकता वा पासपोर्ट नम्बर वा जन्ममिति वा पासवर्ड वा चालक अनुमती नम्बर वा तस्बिरहरू पर्दछन जसलाई प्रयोग गरेर सिमकार्ड वा अनलाइन सेवा वा सोसल मिडियामा नक्कली खाता खोल्न मिल्दछ।

८. **बाल यौनदुराचार र अश्लीलता:** बाल यौनदुराचार वा बालबालिका पीडित भएको अश्लील सामग्रीको उत्पादन वा आदानप्रदान परम्परागत कसूर हो र इन्टरनेटको विकासले यो कसूरलाई झनै विस्तृत बनाएको छ। बाल यौन दुराचार अन्तर्गत कम्प्युटर प्रणालीमार्फत वितरण गर्ने उद्देश्यले बाल यौन दुराचारसम्बन्धी सामग्री उत्पादन गर्ने, कम्प्युटर प्रणालीमा त्यस्तो सामग्री प्रस्ताव गर्ने वा उपलब्ध गराउने, कम्प्युटर प्रणालीमार्फत त्यस्तो सामग्री वितरण वा प्रसारण गर्ने, कम्प्युटर प्रणालीमार्फत आफु वा अन्य व्यक्तिका लागि त्यस्तो सामग्री प्राप्त गर्ने तथा कम्प्युटर प्रणाली वा कम्प्युटर डाटा संग्रह गर्ने उपकरणमा त्यस्तो सामग्री राख्ने लगायतका कार्यहरू पर्दछन्। अश्लील सामग्रीको उत्पादन वा वितरण वा प्रयोगलाई कानुनी मान्यता भएका देशहरूमा पनि त्यस्ता कार्यमा बालबालिकाको प्रयोग वा बाल यौनदुराचार सामग्रीलाई गम्भीर प्रकृतिको कसूर मानिन्छ।

९. **गैर कानुनी विषयबस्तु**: साइबर कसूरकै रुपमा गैर कानुनी विषयवस्तुलाई पनि लिने गरिएको छ। गैरकानुनी विषयवस्तु भन्नाले इन्टरनेटमा प्रकाशन वा प्रसारण गर्न नहुने भनी रोक लगाइएका विषयवस्तु पर्दछन् र त्यस्तो सामग्री प्रकाशन गरेमा सजायको समेत व्यवस्था गरिएको हुन्छ।

२.१.५ विद्युतीय कसूरदारका किसिम (Type of Offender)

हालसम्मको अनुभव र प्रवृत्तिका आधारमा निम्न प्रकारका विद्युतीय कसूरदारहरूको पहिचान भएको देखिन्छ।

१. Insider Threats: कुनै संघसंस्था वा निकायमा काम गर्ने त्यस्ता छद्म व्यक्तिहरू जसले आर्थिक वा राजनीतिक कारणले आफ्नै संस्थाको विद्युतीय प्रणालीमा नोक्सान पुऱ्याउँछन् वा गोपनीयता भंग गर्छन्।

२. Hackers: अरूको कम्प्युटर प्रणालीमा घुसपैठ गर्ने, त्यसलाई काम नलाग्ने बनाइदिने वा पासवर्ड चोरी गरेर सूचना सार्वजनिक गर्ने व्यक्तिहरू Hackers हुन्। असल प्रयोजनका लागि वा कुनै प्रणालीको सुरक्षास्थिति जाँच गर्नेहरूलाई Ethical Hacker समेत भन्ने गरिन्छ।

३. Hacivists:राजनीतिक प्रचारबाजीका लागि संस्थापन पक्षको कम्प्युटर प्रणालीमा अनाधिकृत पहुँच पुऱ्याई प्रचारसामग्री फैलाउने व्यक्तिहरू Hacivists हुन्।

४. Virus Writers:भाइरस,मालवेयरजस्ता सफ्टवेयर तयार गर्ने व्यक्तिहरू लाई Virus Writers भनिन्छ।[३]

५. Sensitive Intruders: कसैको कम्प्युटर वा नेटवर्कमा अनाधिकृत प्रवेश गरी संवेदनशील सूचना वा तथ्यांक प्राप्त गर्नेहरू Sensitive Intruders हुन्।[४]

६. Cyber Warriors: कुनै राष्ट्रविरूद्ध अर्को राष्ट्रले योजनाबद्ध रूपमै उक्त राष्ट्रका विद्युतीय प्रणालीहरू ध्वस्त पार्ने र गोपनीय सूचना प्राप्त गर्ने कार्यको लागि खटाएका व्यक्तिहरू Cyber Warrior हरू हुन्। हाल उत्तर कोरियाले अमेरिका लगायतका मुलुकमा यस्तै साइबर लडाकुहरू तैनाथ गरेको आरोप लाग्ने गरेको छ।

७. Terrorists : सरकारी कामकाज र सेवाप्रवाहमा अवरोध ल्याउने वा जनतालाई आतंकित पार्ने काममा कम्प्युटर प्रणालीको दुरूपयोग गर्ने व्यक्तिहरू Terrorists हुन्।

२.१.६ साइबर कसूरको कारण (Reason of Cyber Crime)

साइवर कसूर बढ्नुको कारणहरूलाई यस प्रकार उल्लेख गर्न सकिन्छ।

१. व्यक्तिमा साइवर कसूर सम्बन्धी चेतनाको कमी रहनु,
२. प्रविधिबारे अल्प ज्ञान तर प्रविधिको बढ्दो प्रयोग गर्ने प्रवृत्ति रहनु,
३. प्रविधि प्रयोगको सम्बन्धमा होसियारी अपनाउनु भन्दा लापरवाही गर्ने प्रवृत्ति बढी रहनु,
४. व्यक्तिमा छिटो समयमा धेरै पैसा कमाउने मोह बढेर जानु,
५. साइवर कसूर न्यूनिकरणका लागि समयानुकूल कानुनको अभाव रहनु,
६. व्यक्तिमा नैतिकता, निष्ठा, आध्यात्मिकता आदी गुणको ह्रास हुदै जानु।

२.१.७ साइबर कसूरको प्रकृति (Nature of Cyber Crime)

साइवर कसूरको प्रकृतीलाई यस प्रकार उल्लेख गर्न सकिन्छ।

---

३ रत्नबहादुर बागचन्द, साइबर अपराध र हाम्रो न्यायिक अभ्यास : एक विश्लेषण, प्रतिपादन (२०७३), पृष्ठ १–१७, राष्ट्रिय न्यायिक प्रतिष्ठान, काठमाडौं.

४ ऐ.ऐ.

१. साइबर कसूर अन्तरदेशीय कसूर हो।
२. यो कसूर सम्बन्धित स्थानमा उपस्थित नभई गर्ने गरिने कसूर हो।
३. साइबर कसूर इन्टरनेट जडित कम्प्यूटर नेटवर्कहरूको माध्यमबाट गरिन्छ।
४. इन्टरनेटको गतिको आधारमा साइवर कसूरको लागि लाग्ने समय निर्भर रहन्छ। Fast Internet भएकोमा साइवर कसूर गर्नको लागि कम समय लाग्छ।

२.१.८ साइबर कसूरको तत्वहरू (Elements of Cyber Crime)

साइबर कसूरको लागि आपराधिक मनसाय र आपराधिक कार्य दुबैको विद्यमानता आवश्यक रहेको छ। साइबर कसूरको कसुर स्थापित हुनको लागि शंकारहित तबरबाट आपराधिक मनसाय र आपराधिक कार्य पुष्टी हुन आवश्यक छ।[५]

१. Doctrine of Mens Rea in Cyber Crime: कठोर दायित्व (Strict Liability) आकर्षित हुने कसूरहरू बाहेकको अवस्थामा Mens Rea कसूरको एक अनिवार्य तत्व हो। साइबर कसूरमा Mens rea लाई इंगित गर्न भने गाह्रो हुन्छ। साइबर कसूरमा Mens Rea पुष्टि हुनको लागि निम्न अवस्था प्रमाणित हुनु पर्छ।
   - कम्प्युटर प्रविधीमा अनधिकृत रूपमा पहुँच स्थापित गरेको हुनु पर्छ।
   - पहुँचको सम्बन्धमा निज जानकार रहेको हुनु पर्छ।

२. Doctrine of Actus Rea in Cyber Crime: साइबर कसूरमा अपराधीले सम्पूर्ण कसूर अमूर्त परिवेशमा गर्ने गरेको हुँदा Actus Reus प्रमाणित गर्नु चुनौतीपूर्ण रहेको छ। केही घटनाहरूमा अपराधीले कसूरको क्रममा कसूरसँग सम्बन्धित केही प्रमाण हरू (Footmarks) छोड्न सक्छ। तथापी ति प्रमाणहरू भौतिक रूपमा उपलव्ध हुन सक्ने कम मात्र सम्भावना रहेको हुँदा अदालतमा प्रमाणित गर्न गार्‌हो हुन्छ। साइबर कसूरमा Actus Rea पुष्टि हुनको लागि निम्न अवस्थाको विद्यमानता हुनु पर्छ।
   - कम्प्युटरको प्रयोग गरेर आपराधिक गतिविधिहरू गरेको वा सो को लागि कोशिस गरेको,
   - कम्प्युटरमा भण्डार गरिएको डाटामा पहुँच गरेको वा सो को लागि कोशिस गरेको,
   - कम्प्युटरमा बाहिरबाट Hacking गरेर डाटामा गरेको वा सो को लागि कोशिस गरेको।

२.१.९ साइबर सुरक्षाको परिचय (Introduction of Cyber Security)

साइबर सुरक्षा भन्नाले प्रयोगमा रहेका विभिन्न सूचना प्रणाली र कम्प्यूटर सञ्जाललाई साइबर आक्रमणबाट जोगाउन अवलम्बन गरिने विधि वा प्रक्रिया वा अभ्यास भनेर बुझ्न सकिन्छ। अर्थात प्रयोगमा रहेका मोबाइल, कम्प्यूटर, सर्भर र यस्तै अन्य ईलेक्ट्रोनिक उपकरणहरू र यी उपकरणहरूमा रहेका डाटाको सुरक्षाको निम्ती अपनाउने प्रक्रिया साइबर सुरक्षा हो। यसरी साइबर सुरक्षा एउटा बृहत क्षेत्र हो जसमा मुख्य गरी कम्प्यूटर नेटवर्क सुरक्षा (Computer Network Security), सूचना प्रणाली सुरक्षा (Application or Information System Security) र सूचना सुरक्षा (Information Security) जस्ता क्षेत्रहरू समेटियका हुन्छन्।

५ file:///C:/Users/user/Downloads/३१९-१३-२२३१-१-१०-२०२००१२१.pdf (Assessed on February १०, २०२४)

२.१.१०. साइबर कसूरहरूको न्यूनिकरणका लागि साइबर सुरक्षा

विशेष गरी साइबर सुरक्षा र साइबर कसूर दवै विपरिथार्त शब्दहरू हुन्। साइबर सुरक्षा रक्षात्मक संयन्त्र (Defensive Mechanism) हो जस्तै घरमा चोरी नहोस भनी प्रयोग हुने ताल्चा, जहा साइबर कसूर भन्नाले यस रक्षात्मक संयन्त्रलाई विभिन्न गलत प्रयोजन (Malicious) का लागी तोड्ने प्रयास भनी बुझ्नु पर्दछ।

त्यसैले, साइबर कसूर तथा साइबर कसूरको न्यूनीकरणका गर्न साइबर सुरक्षा विद्यमान छ भने साइबर सुरक्षा जति बलियो हुन्छ, साइबर अपराधीहरूलाई सफल हुन त्यति नै गाह्रो हुन्छ। साइबर सुरक्षाका विशेष पक्षहरू तल उल्लेख गरिएका छन्।

२.१.११.सक्षम साइबर सुरक्षा संयन्त्रका मुल स्तम्भहरू (Main Pillars):

प्रभावकारी साइबर सुरक्षाको विकासका लागि साधारणतया तल उल्लेखित मुख्य दुई वटा अवधारणाहरूको प्रयोग गरिएको पाइन्छ।

१. **The CIA triad:**

यस अवधारणाले सूचना सुरक्षाका मुख्य तीनवटा पक्षहरूमा जोड दिएको हुन्छ।

(१) गोपनियता (Confidentiality): सूचनाको पहुँच वा जानकारी आधिकारिक प्रयोगकर्ताहरूलाई मात्र छ भनी सुनिश्चित गर्ने।

यसले वित्तीय रेकर्डहरू, व्यक्तिगत जानकारी, वा व्यापारका गोप्य संवेदनशील डाटाहरूलाई अनधिकृत पहुँचबाट जोगाउँछ। फायरवाल (Firewall), इन्क्रिप्शन (Encryption), र पहुँच नियन्त्रण (Access Control) हरू जस्ता प्रविधिहरूले गोपनीयतामा योगदान गर्दछ।

(२) अखण्डता (Integrity): डाटा र प्रणालीहरूको शुद्धता र पूर्णताको ग्यारेन्टी गर्ने।

यसले संयोगवश वा दुर्भावनापूर्ण रूपमा सूचनालाई परिवर्तन वा नष्ट हुनबाट जोगाउँछ। ब्याकअप (Backup), डाटा प्रमाणीकरण (Data Validation), र घुसपैठ पत्ता लगाउने प्रणालीहरू (Intrusion Detection Systems) ले अखण्डता कायम राख्न मद्दत गर्दछ।

(३) उपलब्धता (Availability): आधिकारिक प्रयोगकर्ताहरूलाई सूचनाको पहुँच समयमै अर्थात चाहिएको बखत प्रदान गर्ने र भरपर्दो छ भनी सुनिश्चित गर्ने।

(४) रिडन्डन्सी (Redundancy), प्रकोप रिकभरी योजनाहरू (Disaster Recovery Plans), र अपटाइम निगरानी (Uptime Monitoring) जस्ता प्रविधिहरुको प्रयोगले उपलब्धतामा योगदान गर्दछ।

२. **The pillars of information assurance:**

यस अवधारणाले CIA triad लाई विस्तार गरी थप दुई पक्षहरू समावेस गरेको छ।

(१) प्रमाणिकता (Authenticity): स्रोत वा डाटाको वैधता प्रमाणित गर्ने।

यसले प्रयोगकर्ता (User) वा यन्त्रहरू (Devices) जसले दाबी गर्छ उसकै हो भनी प्रमाणित गर्छ। पासवर्ड

(Password), Multifactor Authentication र Digital Certificate जस्ता प्रविधिहरूको प्रयोगले प्रमाणिकता प्रदान गर्दछन्।

(२) गैर खण्डन (Non-repudiation): सूचना प्रणालीको प्रयोगका दौरान गरिने क्रियाकलाप कुन प्रयोगकर्ताबाट उत्पन्न भएको हो भन्ने प्रमाण प्रदान गर्ने। जसकारण भोली गएर उक्त प्रयोगकर्ताले मैले यो गरेको होइन भनी भन्न सक्ने छैन्। यो वित्तीय लेनदेन वा कानुनी कागजातहरू जस्ता गतिविधिहरूको लागि महत्त्वपूर्ण छ भने डिजिटल हस्ताक्षर (Digital Signature) र लेखापरीक्षण लगहरू (Audit Log) मार्फत प्राप्त गर्न सकिन्छ। एक प्रभावकारी साइबर सुरक्षा संयन्त्रले यी सबै स्तम्भहरूलाई राम्रोसँग एकिकृत रूपमा प्रयोग हुने गरी सम्बोधन गर्नुपर्छ, किनभने यी सबै स्तम्भहरू एक आर्काका परिपुरूक हुन्। जस्तै बलियो Access Control ले गोपनियता (Confidentiality) मा सहयोग दिनुका साथै डाटा परिमार्जन गर्न रोक्नका साथै परिमार्जन गर्न सफल भए पनि को कसले गर्‌यो सो को लेखाजोखा समेत व्यवस्थापन गर्ने भएकोले अखण्ता (Integrity) मा समेत सहयोग गर्दछ।

यसरी नेपालमा E-Governance सेवा प्रदान गर्ने जुनसकै संघ संस्थाले माथी उल्लेखित सूचना सुरक्षाका लागि विशेष ध्यान दिनु पर्ने स्तम्भ (Pillar) हरूको व्यवस्थापन गरेको हुनुपर्छ साथै गरे नगरेको अनुगमन तथा कार्यान्वयन गर्नका लागि कुनै तेस्रो संस्थालाई जिम्मेवारी दिनु पर्ने नित्तान्त जरूरी देखिन्छ।

२.१.१२. साइबर कसूर र AI

एआई कम्प्युटर विज्ञानको एक क्षेत्र हो, जसले मानिसको दिमागको प्रयोग गर्छ। एआई सिस्टम आफैं चल्दैन, यसमा डेटा अर्थात् सूचना तथा तथ्याङ्क हाल्नुपर्छ, जसको एक खालको 'डेटा सोर्स' (तथ्याङ्ककको स्रोत) हुन्छ। अनि एआई सिस्टमले त्यसलाई प्रोसेस (प्रशोधन) गर्छ। सुरुमा तालिम दिएको तरिकाबाट मोडेल बनाउँछ र डेटाको हिसाबले परिणाम दिन्छ, अन्तरक्रिया गर्छ वा मानव दिमागको नक्कल गर्छ। एआईमा जति धेरै डेटा हालिन्छ, त्यो त्यति नै राम्रो बन्दै जान्छ। तर सबै एआई सिस्टमहरूका लागि ठूला डेटा सोर्सको आवश्यकता पर्दैन। खासमा 'बिग डेटा (ठूला तथ्याङ्क) एआईको अति महत्त्वपूर्ण पक्ष हो। एआईलाई काम गर्नको लागि मुख्य चार प्रक्रियाको आवश्यकता पर्छ, मसिन लर्निङ, न्युरल नेटवर्क, डेटा तथा डेटा प्रोसेसिङ र एल्गोरिदम।[६]

१. मसिन लर्निङ (एमएल):

मसिन लर्निङ (एमएल)लाई फाउन्डेसन अफ एआई अर्थात् एआईको जग भनिन्छ। यसको सोझो मतलब हुन्छ; मसिनलाई मानिसको दिमागले कसरी काम गर्छ भनेर सिकाउनु। यसका लागि मसिन लर्निङ टुलमा जति डेटा हालिन्छ, तिबाट एआई सिस्टम, डेटा सेट निर्माण हुन्छ। मसिन लर्निङको प्रक्रियाबाट डेटाबाट एआई सिस्टमको सिकाइ हुन्छ। तर डेटा प्रोसेस गर्नको लागि डेटाबाट उपयोगी जानकारी निकाल्नको लागि सफ्टवेयर प्रोग्राम र एल्गोरिदमको आवश्यकता त पर्छ नै। अब डेटा यति धेरै मात्रामा हुन्छ कि, त्यसलाई डेटाको पिरामिड नै पनि भन्न सकिन्छ। यही डेटालाई प्रोसेस गर्नको लागि गणितीय मोडेलको आवश्यकता पर्छ। 'इमेज क्लासिफिकेसन' यसको एउटा उदाहरण हो। जस्तै तपाईं कतिपय वेबसाइटमा जानुहुन्छ, त्यहाँ धेरै फोटोहरूमध्ये जसमा ट्राफिक लाइट देखाइएको हुन्छ, त्यसलाई छनौट गर्न भनिन्छ। जुन फोटोमा बिरालो बनेको छ, त्यसलाई पहिचान गर्नुहोस्

६ *कसरी बनाइन्छ एआई प्रविधि अनि कसरी गर्छ काम* ?, हेर्नुहोस: https://techpana.com/२०२४/१४६१६०/how-is-ai-technology-made-and-how-does-it-work

भनिन्छ । तपाईंले सही फोटो छान्नु भएको छ वा छैन भन्ने सिस्टमलाई कसरी थाहा हुन्छ ? हो, यही हो मसिन लर्निङ ।

२. न्युरल नेटवर्क:

एआईको अर्को महत्त्वपूर्ण अङ्ग हो, न्युरल नेटवर्क, जसलाई 'विल्डिङ ब्लक्स अफ एआई' पनि भनिन्छ । खासमा एआई सिस्टमको मसिन लर्निङ न्युरल नेटवर्कको कारण हुन्छ । जुन जैविकताबाट प्रेरित न्युरल नेटवर्क आर्किटेक्चर हो । जसरी मानिसको दिमागका न्युरोनहरू अर्थात् नसाहरू आपसमा जोडिएका हुन्छन्, त्यसै गरी न्युरल नेटवर्कमा अनेक थरीका हिडन लेयर्स (अदृश्य तहहरू) हुन्छन् । तिनै तहहरू बीचबाट गुज्रिँदै डेटा प्रोसेस (प्रशोधन) हुन्छ ।

३. डेटा प्रोसेसिङ

तहगत रूपमा डेटा गुज्रिंदा मसिनको डिप लर्निङ चरणमा प्रवेश गर्छ । यसमा सबै डेटामा रहेको कनेक्सनलाई जोड्दै जाँदा एआई सिस्टमले राम्रो परिणाम दिन्छ ।

यसको तरिका निम्न अनुसार हुन्छ;

पहिले इन्पुट (डेटा भित्रिने) तहले डेटा प्राप्त गर्छ । हिडन लेयर (अदृश्य तह) ले डेटालाई प्रोसेस (प्रशोधन) गर्छ । आखिरमा आउटपुट लेयर (बाहिरिने तह) मार्फत परिणाम निस्किन्छ । आर्टिफिसियल इन्टेलिजेन्सको लागि सबैभन्दा महत्त्वपूर्ण डेटा नै हुन्छ । डेटालाई 'फ्युल फर एआई सिस्टम' (एआई प्रणालीको इन्धन) पनि भनिन्छ । किनकि एआई मोडेललाई सिकाउनको लागि बिना डेटा सेट केही गर्न सकिंदैन । यस्तो डेटा सेटमा अनेक थरीका विशेषता हुन जरुरी हुन्छ । जस्तो कि डेटा पूर्ण हुनुपर्छ, कुनै पनि डेटा हराएको हुनुहुँदैन । एआई सिस्टमले काम गर्नको लागि डेटाको निरन्तरता पनि चाहिन्छ । डेटा सही एवं तथ्यपरक हुनुपर्छ । त्यसमा कुनै पनि गलत डेटा हुनुहुँदैन । साथै डेटा अद्यावधिक भएको पनि हुनुपर्छ । एआई सिस्टमलाई तालिम दिनको लागि सामान्यतया तीन प्रकारको डेटा इनपुट दिनुपर्छ, जस्तै- स्ट्रक्चर्ड, अनस्ट्रक्चर्ड र सेमी-स्ट्रक्चर्ड डेटा ।

स्ट्रक्चर्ड डेटामा मितिहरू, स्थानहरू, क्रेडिट कार्ड नम्बरहरू, नम्बर सिरिज वा अन्य स्ट्यान्डर्ड इनपुट विधिहरू पर्छन् । स्ट्रक्चर्ड डेटामा डेटा जहिले पनि स्ट्यान्डर्ड फर्म्याटमा हुन्छ । अनस्ट्रक्चर्ड डेटामा कुनै विशेष डेटा वा सूचना हराएको हुन्छ । अनस्ट्रक्चर्ड टेक्स्ट, फोटो, भिडिओमा एआई सिस्टमले प्याटर्न खोज्ने कोशिस गर्छ । यसको लागि एआई सिस्टमले एनएलपी (नेचुरल ल्याङ्गेवज प्रोसेसिङ), कम्प्युटर भिजन वा अन्य तरिकाबाट डेटाको प्रोसेस गर्छ ।

एआई सिस्टमसँग कुनै पनि प्रि-डिफाइन्ड (पहिले नै परिभाषित) मोडेल नहुँदा सेमी-स्ट्रक्चर्ड डेटाको प्रयोग हुन्छ । यो तरिकामा डेटाले 'जेएसओएन', 'एक्सएमएल' र 'सीएसभी' फर्म्याट प्रयोग गर्छन् । यो तरिका अपनाउँदा अनस्ट्रक्चर्ड डेटा सोर्सको लाभ लिन पाइन्छ र तालिमका लागि प्राप्त डेटालाई स्टोर गर्न सहज हुन्छ ।

४. एल्गोरिदम

आर्टिफिसियल इन्टेलिजेन्सको अन्तिम महत्त्वपूर्ण अङ्गको रूपमा समस्या निराकरणको काम एल्गोरिदमले गर्छ। एल्गोरिदमलाई एआईको 'ब्याकबोन' अर्थात् मेरुदण्ड पनि भनिन्छ। खासमा एल्गोरिदम्स गणितीय प्रक्रिया हो, जसमा एआई सिस्टमले कसरी सिक्छ, निर्णय लिने क्षमता कसरी सुधार गर्न सक्छ र समस्याको निराकरणलाई कसरी व्यवस्थापन गर्छ भन्ने कुरा रहेको हुन्छ। एल्गोरिदमबाट नै कच्चा डेटा काम लायक डेटामा परिणत हुन्छ अनि ग्राहक र कम्पनीको काममा आउँछ।

साइबर कसूरमा कृत्रिम बुद्धिमत्ता (AI) को प्रयोगले अपराधीहरूलाई आक्रमणहरू थप परिष्कृत, प्रभावकारी, र कठिन पार्न मद्दत गरिरहेको छ। साइबर कसूरमा AI को प्रयोग निम्नानुसार रहेको पाइन्छ।

१. स्वचालित आक्रमणहरू (Automated Attacks)

AI को प्रयोगले साइबर अपराधीहरूलाई स्वचालित रूपमा आक्रमणहरू गर्न सक्षम बनाउँछ। यसले निम्नलिखित क्रियाकलापहरूमा समावेश गर्दछ:

- स्वचालित स्क्यानिङ: AI उपकरणहरूले स्वचालित रूपमा नेटवर्क र सिस्टमहरूमा कमजोर बिन्दुहरू खोज्न सक्छन्। उदाहरणका लागि, AI ले पत्तालगाउँछ कि कुन सफ्टवेयर संस्करण पुरानो छ र ज्ञात कमजोरीहरू छन्।
- प्याचिंग असिस्टेन्ट्स: AI ले कमजोर सफ्टवेयरको सूची बनाई यसलाई एक्सप्लॉइट गर्न आवश्यक मालवेयरहरू तयार गर्न सक्छ।

२. स्पीयर फिसिङ (Spear Phishing)

AI ले स्पीयर फिसिङ आक्रमणहरूलाई अझ बढी परिष्कृत बनाउँछ:

- पर्सनलाइज्ड फिसिङ इमेल: AI ले सामाजिक मिडिया र अन्य अनलाइन स्रोतहरूबाट जानकारी संकलन गरेर व्यक्तिगत र विश्वसनीय फिसिङ इमेलहरू तयार गर्न सक्छ। यसले पीडितलाई विश्वास गराउन सजिलो बनाउँछ।
- भ्वाइस फिसिङ: AI को प्रयोगले भ्वाइस क्लोनिङ गरी टार्गेट व्यक्तिको आवाजको नक्कल गर्न सकिन्छ र फोन कलमार्फत संवेदनशील जानकारी लिने प्रयास गर्न सकिन्छ।

३. मालवेयर उत्पन्न गर्नु (Generating Malware)

AI ले मालवेयरलाई थप खतरनाक बनाउन सक्छ:

- पोलिमोर्फिक मालवेयर: AI ले लगातार आफ्नो कोड परिवर्तन गर्ने मालवेयर उत्पन्न गर्न सक्छ जसले गर्दा परम्परागत एंटीभाइरस सफ्टवेयरहरूले यसलाई पहिचान गर्न गाह्रो हुन्छ।
- एडभान्स्ड पर्सिस्टेन्ट थ्रेट्स (APT): AI ले लक्ष्यको नेटवर्कमा लामो समयसम्म अनदेखा रहन सक्ने मालवेयर बनाउन सक्छ, जसले संवेदनशील डेटा चोर्न सक्छ।

४. क्याप्चा समाधान गर्नु (Captcha Solving)

क्याप्चा बाइपास गर्ने AI को उपयोग:

- इमेज रेकग्निशन: AI इमेज रेकग्निशन प्रविधिको प्रयोग गरेर क्याप्चाहरूलाई सही रूपमा हल गर्न सक्छ।
- नेचुरल लैंग्वेज प्रोसेसिंग (NLP): NLP प्रविधिको प्रयोग गरेर टेक्स्ट बेस्ड क्याप्चाहरूलाई सजिलै हल गर्न सकिन्छ।

५. बोटनेटहरू (Botnets)

AI को प्रयोग बोटनेटहरूमा निम्नानूसारको कार्य गर्दछ।

- स्मार्ट बोटनेट व्यवस्थापन: AI ले बोटनेटको हरेक बोटलाई स्वतः अपडेट र व्यवस्थापन गर्न सक्छ, जसले बोटनेटलाई अझ कुशल र लचिलो बनाउँछ।
- ट्राफिक एनालिसिस: AI ले ट्राफिक विश्लेषण गरेर बोटनेटको आक्रमणको प्रभावकारिता बढाउन सक्छ।

६. सोसल इन्जिनियरिङ (Social Engineering)

AI को प्रयोगले सामाजिक इन्जिनियरिङ आक्रमणहरूलाई थप प्रभावकारी बनाउँछ:

- डेटा माइनिङ: AI ले विशाल मात्रामा डेटा विश्लेषण गरेर पीडितको व्यवहार र प्राथमिकताहरूको बारेमा जानकारी प्राप्त गर्न सक्छ।
- च्याटबोटहरू: AI आधारित च्याटबोटहरूले वास्तविक व्यक्तिको जस्तो व्यवहार गरेर पीडितबाट संवेदनशील जानकारी निकाल्न सक्छ।

७. एआई आधारित साइबर हमला टूल्स (AI-based Cyber Attack Tools)

कुनै पनि जटिल साइबर आक्रमणहरूलाई स्वचालित र अनुकूलित गर्न AI आधारित उपकरणहरूको प्रयोग:

- आक्रामक AI: AI ले सुरक्षा प्रणालीहरूलाई छल्न अनुकूलित आक्रमण रणनीतिहरू विकास गर्न सक्छ।
- डीपफेकहरू: AI को प्रयोगले डिपफेक भिडियोहरू र आवाजहरू बनाउने जसले नक्कली समाचार, ब्ल्याकमेल र अन्य किसिमका साइबर कसूरहरूलाई सजिलो बनाउँछ।

साइबर कसूरमा AI को प्रयोगले साइबर हमलाहरूलाई थप खतरनाक, प्रभावकारी, र कठिन पारिरहेको छ। यो प्रवृत्ति निरन्तर बढ्दै जान्छ, जसले साइबर सुरक्षाका क्षेत्रमा नयाँ चुनौतीहरू र उपायहरूको विकास आवश्यक बनाउँछ।

२.२ साइबर कसूर सम्बन्धमा अन्तर्राष्ट्रिय कानुनको विकासक्रम (Development of International Law on Cyber Crime)

सन् १९६० मा Roy N. Freed द्वारा लिखित A Lawyer's Guide through the Computer Maze प्रकाशित भयो। जसलाई विश्वमा कम्प्युटर कानुनको बारेमा प्रकाशित पहिलो आलेखको रूपमा मानिन्छ। [७] साइबर कसूर सम्बन्धमा अन्तराष्ट्रिय कानूनको सम्बन्धमा अध्ययन गर्दा मानव अधिकार सम्बन्धी विश्वव्यापी घोषणापत्र, १९४८ र

७ ऐ. ऐ.पृष्ठ ५६

नागरिक तथा राजनीतिक अधिकारसम्बन्धी अन्तर्राष्ट्रिय अनुबन्ध, १९६६ लाई महत्वपूर्ण दस्ताबेजको रूपमा लिन सकिन्छ। मानव अधिकार सम्बन्धी विश्वव्यापी घोषणापत्र, १९४८ले सर्वप्रथम मानव अधिकारको विषयमा लिपीबद्ध गर्ने काम गर्‌यो भने नागरिक तथा राजनीतिक अधिकारसम्बन्धी अन्तर्राष्ट्रिय अनुबन्ध, १९६६ को धारा १९ मा प्रत्येक व्यक्तिलाई अभिव्यक्ति स्वतन्त्रताको अधिकार हुनेछ, जस अन्तर्गत बिना कुनै वन्देज वा सीमा आफूले चाहेको सूचना तथा विचार खोज्ने, प्राप्त गर्ने तथा त्यस्तो सूचना वा विचार मौखिक, लिखित वा मुद्रित रूपमा वा कलात्मक रूपमा वा आफ्नो छनौटको अन्य कुनै माध्यमद्वारा प्रसार गर्न पाउने स्वतन्त्रता हुने उल्लेख गरि व्यक्तिलाई अभिव्यक्ति स्वतन्त्रताको स्थापना गरिदिएको पाइन्छ।

सन् १९७० देखि मुलुकहरूले व्यक्तिको गोपनीयता संरक्षण गर्न गोपनियता सम्बन्धी कानुन निर्माण गर्न थाले। Organization for Economic Cooperation and Development र Council of Europe का Model Laws मा आधारित भएर यी कानुनहरू तयार भए। तत्कालीन पश्चिम जर्मनीले १९७० मा पहिलोपटक Data Protection Law तर्जुमा गर्‌यो।[८] त्यसपछि स्वीडेन (१९७३), अमेरिका (१९७४), पूर्वी जर्मनी (१९७७) र फ्रान्स (१९७८) ले समेत तथ्यांक संरक्षणमा कानुनी व्यवस्था गर्न थाले। विशुध्द कम्प्युटर कारोबारमै केन्द्रित कानुन बनाउने श्रेय भने संयुक्त राज्य अमेरिकालाई जान्छ जसले सन् १९८४ मा Computer Fraud and Abuse Act बनाई लागू गर्‌यो जुन अद्यापि बहाल छ।[९] विश्वमा साइबर कसूर सबैभन्दा बढी हुने मुलुकको सूचीमा अमेरिका पहिलो स्थानमा आउँछ।

यसै सन्दर्भमा विश्वभरिका विद्युतीय कानुनहरूमा एकरूपता ल्याउनका लागि United Nations Commission on International Trade Law (UNCITRAL) ले सन् १९९६ मा Model Law on Electronic Commerce र २००५ मा Model Law on Electronic Signature जारी गर्‌यो। यसैगरी, WIPO Copyright Rules, १९९६ र WIPO Performance and Phonograms Treaty Rules, १९९६ हरूले मूलत: प्रतिलिपि अधिकारसँग सम्बन्ध राख्ने भएता पनि विद्युतीय माध्यमबाट प्रतिलिपि अधिकार उल्लंघन गरेकोमा उपचारको व्यवस्था गरेकोले यसलाई पनि सान्दर्भिक रूपमा लिन सकिन्छ। यस क्रममा, अक्टोबर २४, १९९९ मा Internet Corporation for Assigned Names and Numbers ले डोमेन नेमका विवादहरू हल गर्न Uniform Domain Name Dispute Resolution Policy जारी गर्‌यो।[१०]

विश्वमा इन्टरनेटको आरम्भ सन् १९९० को दशकमा भएता पनि कम्प्युटर र इन्टरनेटजन्य कसूरलाई सम्बोधन गर्ने पहिलो क्षेत्रीय महासन्धिको रूपमा युरोपेली युनियनभर सन् २००१ देखि लागू भएको Budapest Convention on Cyber Crime लाई लिन सकिन्छ।[११] यस विषयमा पहिलो अन्तर्राष्ट्रिय महासन्धि हालसम्म तयार भएको देखिँदैन। क्षेत्रीय सन्धिकै निरन्तरतास्वरूप जून २०१० मा ५ वटा पूर्वी अफ्रिकी मुलुकहरू बुरूण्डी, केन्या, रूवाण्डा, तान्जानिया र युगाण्डा मिलेर साइबर कसूरको नियन्त्रणका लागि Framework for Cyber Laws मस्यौदा गरी कार्यान्वयनमा ल्याए।[१२] विश्वका कुल साइबर कसूरमध्ये करिब २३ प्रतिशत अमेरिकामा हुन्छन् भने दोस्रो चीनमा ९ प्रतिशत र तेस्रो जर्मनीमा ६ प्रतिशत हुने गरेको सिमेन्टकको अध्ययनले देखाएको छ।[१३]

८ ऐ. ऐ.पृष्ठ ५७
९ ऐ. ऐ.पृष्ठ ५७
१० ऐ. ऐ.पृष्ठ ५७
११ ऐ. ऐ.पृष्ठ ५८
१२ ऐ. ऐ.पृष्ठ ५९
१३ गोकर्ण प्रसाद उपाध्याय, बढ्दो साइवर अपराधको जोखिम, http://www.karobardaily.com/news

२.३ साइबर सुरक्षा र कसूर सम्बन्धी केही देशको कानून र नीति तथा अभ्यासहरू (International Policies, Laws and Practices)

भारत, संयुक्त राज्य अमेरिका,संयुक्त अधिराज्य, कोरिया र सिंगापुरमा साइवर कसूर सम्बन्धमा भएको अभ्यासलाई यहाँ उल्लेख गरिएको छ।

२.३.१. भारत

भारतमा साइवर कसूरको नियन्त्रणको लागि Information Technology (IT) Act, २००० जारी गरी कार्यान्वयनमा ल्याइएको छ । भारतमा साइवर कसूर सम्बन्धी गतिविधिलाई सम्बोधन गर्ने सम्बन्धमा Indian Computer Emergency Response Team (ICERT) को निर्माण गरिएको छ।[१४] यस बाहेक भारतमा कार्यान्वयनमा रहेका भारतीय दण्ड संहिता, १८६०, प्रमाण ऐन, १८७२ तथा फौज्दारी कार्यविधि संहिता, १९७३ लगायतका ऐनमा रहेका प्रावधानहरू पनि साइवर कसूरको विरूद्धमा सम्बन्धित रहेका छन्।

भारतमा सूचना तथा प्रविधिको क्रान्तिले त्यहाँको व्यापारिक कारोबारको तरिका, सरकाद्वारा ल्याइएका विभिन्न कार्यक्रमको परिचालन गर्ने विधिलगायत राष्ट्रियताको रक्षाको विधि नै परिवर्तन भएको पाइन्छ। जब सन् २००९ मा भारतले आधार कार्ड (Aadhar Card) प्रणालीको सुरुवात गर्यो त्यस लगत्तै त्यहाँको सरकारी स्तरबाट प्रदान गरिने सेवाहरूलाई व्यापक रूपमा e- government का विभिन्न कार्यक्रमहरू बनाएर प्रदान गर्न थालियो।

भारतमा सन् १९९० को दशकको मध्यबाट नै e-government को सुरुवात भए तापनि जब जुलाइ १. २०१५ प्रधानमन्त्री नरेन्द्र मोदीले "Digital India" कार्यक्रमको सुरुवात गरे। त्यसपछि भारतमा भएका ग्रामीण इलाकाहरूमा पनि विस्तारै द्रुत गतिको इन्टरनेटको पहुँच हुन थाल्यो। १९ यसपछि आएको National e-governance plan २.० (NEGP-२००६) सँगसँगै यही योजनामार्फत इ क्रान्ति (E-Kranti) को घोषणा गरी अरू थुप्रै सूचना प्रविधिसँग सम्बन्धित योजनाहरूसमेत तर्जुमा भई त्यसको कार्यान्वयन हुन थाल्यो। २० यसरी सूचना प्रविधि र इन्टरनेटको तीव्र विकास र प्रयोग सँगसँगै साइबर सुरक्षासँग सम्बन्धित विभिन्न प्रश्नहरू उठ्न लागे र भारतले त्यसको समाधान र सम्बोधनका लागि सर्वप्रथम त्यहाँको सूचना प्रविधि ऐन, २००० (Information Technology Act, २०००) लाई संशोधन गरी यससँग सम्बन्धित थुप्रै प्रावधानहरू पनि संलग्न गराउने कार्यहरू भएको देखिन्छ। हालाकि साइबर सुरक्षालाई मध्यनजर गरी सो ऐन प्रारम्भ हुने बेलामै समेत केही प्रावधानहरू समावेस थिए। भारतमा साइबर सुरक्षासम्बन्धी भएका महत्त्वपूर्ण प्रावधानहरूलाई यहाँ चर्चा गरिएको छ।

(१) सूचना प्रविधि ऐन, २००० (Information Technology Act, २०००)

सूचना प्रविधि ऐन, २००० भारतको साइबर कानूनको मेरुदण्ड मानिन्छ। जब United Nations Commission on International Trade Law (UNCITRAL) ले १९९६ को Model Law on e- commerce अपनायो र भारतसमेत त्यसको पक्ष राष्ट्र बन्यो। त्यसैका आधारमा भारतले त्यसका प्रावधानहरूलाई आत्मसात् गर्नका लागि सन् २००० मा सूचना प्रविधि ऐन, २००० (Information Technology Act, २००० जारी गर्यो। यो ऐनले मूलतः साइबर सुरक्षासँग सरोकार राख्ने निम्न कुराहरूलाई समेटेको पाइन्छ।

---

१४ file:///C:/Users/user/Downloads/३१९-१३-२२३१-१-१०-२०२००१२१.pdf (Assessed on February १०, २०२४)

- डिजिटल हस्ताक्षर (Digital Signature) को कानूनी मान्यता
- साइबर कसूर तथा उल्लङ्घन र सजाय

साइबर सुरक्षाको दृष्टिकोणबाट डिजिटल हस्ताक्षर (Digital Signature) लाई एउटा महत्त्वपूर्ण पाटोको रूपमा लिइन्छ । डिजिटल हस्ताक्षर र इलेक्ट्रोनिक हस्ताक्षरलाई कसै कसैले समानार्थी शब्दको रूपमा प्रयोग गर्ने गरेको र बुझ्ने गरेकोसमेत पाइन्छ तर त्यस्तो कदापि होइन । प्रिन्ट गरिएको कागजातमा प्रमाणीकरणका लागि हस्ताक्षर प्रयोग भए जस्तै समान प्रयोजनका लागि डिजिटल तथा विद्युतीय सामग्रीमा हुने एक किसिमको हस्ताक्षर नै इलेक्ट्रोनिक हस्ताक्षर हो । हस्ताक्षरको स्क्यान कपि बायोमेट्रिक हस्ताक्षरहरू, रेटिना स्क्यान, फेस रिकग्निसन आदि इलेक्ट्रोनिक हस्ताक्षरका उदाहरणहरू हुन् भने डिजिटल हस्ताक्षर त्यति मात्र नभएर साइबर सुरक्षाको एउटा उपकरण पनि हो । २३ यो एउटा विद्युतीय माध्यमबाट काम कारबाही गर्नका लागि प्रदान एउटा पिन कोड हो । जुन कोडले सूचनाहरू सुरक्षित माध्यमबाट आदानप्रदान गर्न सकिन्छ । यसको प्रयोगबाट अनलाइनबाट हुने कारोबार भरपर्दो र सुरक्षित बनाउन सकिन्छ । डिजिटल हस्ताक्षर प्रयोग गर्नका लागि जोडी साँचो एउटा सार्वजनिक साँचो (Public key) र अर्को निजी साँचो (Private key) को आवश्यकता पर्दछ र यसैको प्रयोगबाट Data हरूको Encryption र Description गरी कारोबार तथा सूचनाहरूलाई सुरक्षित तरिकाबाट पठाउन तथा प्राप्त गर्न सकिन्छ । २४ यसरी भारतको सूचना प्रविधि ऐन, २००० को संशोधनबाट यसलाई अझ बढी व्यवस्थित बनाएको पाइन्छ । डिजिटल हस्ताक्षरको गुणअनुसार नै यसको प्रयोगबाट निम्न तीन बुँदाको सुनिधितता गरिएको हुन्छ ।

- प्रमाणीकरण (Authentication): डिजिटल हस्ताक्षर प्रयोग गरीगरिएको कारोबारमा हस्ताक्षरकर्ताको प्रमाणीकरण प्रदान गर्ने प्रमाणपत्र (Digital Certificate) समेत टाँसिएको हुन्छ जसबाट हस्ताक्षरको प्रमाणीकरण गर्न सकिन्छ ।
- सुनिश्चितता / निष्ठा (Integrity): डिजिटल हस्ताक्षर प्रयोग गरी पठाइएका कागजातहरू सामाग्रीहरू तथा सन्देशहरूको मूल स्रोतको सुनिश्चितता गर्न सकिन्छ ।
- गैर खण्डन (Non-Repudiation): डिजिटल हस्ताक्षर प्रयोग गरी कुनै सन्देश वा कागजात पठाइएको अवस्थामा भविष्यमा उक्त हस्ताक्षर कर्ताले सो हस्ताक्षर गरी पठाएको सन्देश वा कागजात मैले पठाएको होइन भनी अस्वीकार गर्न सक्दैन ।

(२) राष्ट्रिय साइबर सुरक्षा नीति, २०१३ (National Cyber Security Policy-२०१३)

भारतमा बढ्दै गइरहेको साइबरसम्बन्धी कसूर तथा त्यसले असुरक्षित बनाएको साइबर स्पेसलाई त्यहाँका आम जनता, व्यापारहरू तथा सरकारका लागि सुरक्षित बनाउने परिदृष्य (Vision) का साथ सन् २०१३ मा राष्ट्रिय साइबर सुरक्षा नीति लागु गरेको थियो । साइबर स्पेसमा सूचना तथा सूचना पूर्वाधारको सुरक्षा गर्ने, साइबर खतराहरूलाई सम्बोधन गर्न सक्ने गरी र यसबाट बचाउन सक्ने गरी क्षमता विकासका कार्यक्रमहरू सञ्चालन गर्ने, यससँग सम्बन्धित कमजोरीहरू र यसबाट हुने क्षतिसमेतलाई संस्थागत संरचना, जनता, प्रक्रिया, प्रविधि तथा सहकार्यबाट कम गर्दै लैजाने परिलक्ष्य (Mission) समेत यस नीतिले लिएको पाइन्छ ।

Information Technology {The Indian Computer Emergency Response Team (CERT-In) and manner of performing function and duties} Rules, २०१३

भारतमा साइवर सुरक्षासँग सम्बन्धित सम्भावित खतराहरू र सोसँग सम्बन्धित घटनाहरूको तत्काल सम्बोधन गर्ने प्रक्रिया तथा कार्यहरूका सम्बन्धमा व्यवस्था गर्नका लागि सूचना प्रविधि ऐनलाई सघाउने हेतुले यो नियमावली जारी गरेको पाइन्छ। (CERT-In) ले मूलतः सूचना प्रविधिसँग सम्बन्धित विभिन्न संवेदनशील पूर्वाधारहरूको सुरक्षालाई ध्यान दिँदै निम्न कार्यहरू गर्दै आएको पाइन्छ।

- सूचनाहरूको आदान प्रदान, रोकथाम र पूर्वचेतावनी (Early warning),
- सूचना प्रविधिमा केन्द्रित पहिचान (Detection),
- प्रतिक्रिया (Reaction).
- संकट व्यवस्थापन (Crisis Management)।

२.३.२. संयुक्त राज्य अमेरिका

संयुक्त राज्य अमेरिकामा Computer Fraud and Abuse Act, १९८४, Electronic Communications Privacy Act, १९८६, Digital Millenium Copyright Act, १९८८, Electronic Signature in Global and National Commerce Act, २००० लगायतका ऐनहरू साइवर कसूरको नियन्त्रण सँग सम्बन्धित रहेका छन्।[१५]

कम्प्युटर तथा कम्प्युटर प्रणालीसँग सम्बन्धित गतिविधिहरूको नियमन र नियन्त्रण गर्नको लागि अमेरिकामा विभिन्न किसिमका कानूनहरू निर्माण गरी लागु गरेको पाइन्छ। अमेरिकाको संघीय सरकारले प्रत्येक वर्ष सूचना प्रविधि तथा साइबर सुरक्षाको शीर्षकमा सयौं विलियन डलर खर्च गरेको पाइन्छ। "Office of Management and Budget" का अनुसार अमेरिकाको संघीय सरकारले आर्थिक वर्ष २०१६ मा ८२.८ विलियन डलर, आर्थिक वर्ष २०१७ मा ७८.४ विलियन डलर आर्थिक वर्ष २०१८ मा ८१.३ विलियन डलर र आर्थिक वर्ष २०१९ मा ८३.४ विलियन डलर खर्च गरेको पाइन्छ।

(क) The Computer Fraud and Abuse Act, १९८६

The Computer Fraud and Abuse Act, १९८६ लाई अमेरिकाको पहिलो कम्प्युटर तथा साइबर सुरक्षासम्बन्धीको कानूनको रूपमा परिचित छ र जुन ऐन त्यहाँको Comprehensive Crime Control Act, १९८४ को Computer Fraud Law को पाटोलाई प्रतिस्थापन तथा संशोधन गर्ने क्रममा आएको थियो। यसलाई Federal तहको Anti-hacking कानूनको रूपमा चिनिन्छ जसले

कम्प्युटर तथा नेटवर्कको अनधिकृत पहुँचमाथि अंकुश लगाएको पाइन्छ र यसलाई अमेरिकाको फौजदारी कानूनलाई बृहत् बनाउने सिलसिलामा कम्प्युटरसँग सम्बन्धित कसूरहरूलाई समेटेको पाइन्छ। यसको मुख्य कमजोरी कम्प्युटर र नेटवर्कसम्बन्धी ठुला खालका कसूरहरू र साना प्रकृतिका कसूरलाई एउटै आँखाबाट हेरेको पाइन्छ। त्यसैले यससम्बन्धी मुद्दाको अभियोजन तथा फैसलाको क्रममा बृहत् ढंगबाट कानूनी व्याख्या जरुरी थियो। अतः सन् १९९४ मा यसलाई संशोधन गरी फौजदारी घेराबाट समेत बाहिर लगी कम्प्युटरसँग सम्बन्धित देवानी विषयवस्तुहरूसमेतको प्रवेश गराएको पाइन्छ।

१५ https://www.oas.org/juridico/spanish/us_cyb_laws.pdf (Assessed on February ७, २०२४)

(ख) The Clinger - Cohen Act, १९९६

The Clinger-Cohen Act जसलाई Information Technology Management Reform Act का रूपमा पनि चिनिन्छ, यसको माध्यमबाट अमेरिकी संघीय सरकारले अहिलेसम्म अमेरिकाको सूचना प्रविधि (Information Technology) क्षेत्रलाई सूचित व्यवस्थापन गर्दै आएको पाइन्छ । यसको मुख्य गुण भनेको सूचना प्रविधिको क्षेत्रका तोकिएका निकायहरूलाई सूचना प्रविधिसँग सम्बन्धित क्षेत्रमा काम गर्न प्रदान गरेको स्वतन्त्रता हो । यही कारणले गर्दा त्यहाँका सूचना प्रविधि विज्ञहरूले यसलाई अमेरिकाको सूचना प्रविधि विकासको धरोहरका रूपमा लिएकोसमेत पाइन्छ । यसले अमेरिकामा रहेका विभिन्न निकायहरूमा एउटा प्रमुख सूचना अधिकृत रहने परिकल्पना गर्दछ भने उनीहरू आफ्नो निकायमा गर्नु पर्ने सूचना प्रविधिसम्बन्धी योजना तथा सञ्चालनका लागि उत्तरदायीसमेत हुने गर्दछन् ।

(ग) The Federal Information Security Management Act (FISMA), २००२

यस ऐनलाई अमेरिकाका साइबर सुरक्षाको पाटोबाट हेर्दा अत्यन्तै महत्त्वपूर्ण कानूनको रूपमा लिने गरिन्छ । मूलतः अमेरिकी सरकारसँग आवद्ध विद्युतीय सूचनाहरूको सुरक्षा एवंम संरक्षण गर्नका लागि यो कानून जारी गरिएको हो । सरकारसँग रहेका डिजिटल सम्पत्तिहरूलाई प्राकृतिक तथा मानव निर्मित खतराबाट जोगाउनु यो कानूनको मुख्य उद्देश्य हो । यस ऐनले विभिन्न निकायहरूलाई संघीय तहको Data Security का लागि जिम्मेवार गराउदैंछ ।

(घ) The Cyber Security Act of २०१५

तत्कालीन अमेरिकी राष्ट्रपति वाराक ओवामाले जारी गरेको यो कानून अमेरिकाको साइबर सुरक्षाको लागि जारी गरिएका कानूनहरूमध्ये सबैभन्दा अब्बल कानून मानिन्छ । सन् २०१५ को अन्तिम महिनामा यो ऐन जारी गरिएको थियो । यसले विभिन्न निजी क्षेत्रहरू तथा संघीय सरकारका निकायहरूमा साइबर सुरक्षासम्बन्धी सूचनाहरूको सम्प्रेषण गर्ने संयन्त्रहरू तथा यसको कार्यविधिका सम्बन्धमा व्यवस्था गरेको पाइन्छ । ४२ यसले संघीय सरकार बाहिरका अन्य विभिन्न निकायहरूसमेतलाई सूचना प्रणाली (Information System) को Monitor गर्ने, साइबर सुरक्षा प्रयोजनका लागि रक्षात्मक उपाय सञ्चालन गर्नका लागि आधिकारिकता प्रदान गर्ने गर्दछ । ४३ यो ऐनले साइबर सुरक्षासम्बन्धी सूचना सम्प्रेषण तथा वितरण गर्ने केन्द्रीकृत संस्थाको रूपमा Department of Homeland Security (DHS) लाई पहिचान गरेको पाइन्छ ।

(ङ) The Federal Information Security Modernization Act, २०१४ (FISMA २०१४)

यो ऐनले अमेरिकाको Information Security का लागि संघीय तहमा office of Management of Budget (OMB) तथा Department of Homeland Security (DMS) अधिकार तथा जिम्मेवारीको पहिचान गर्ने कार्य गर्दछ ।

(च) The Federal Information Technology Acquisition Reform (FITARA) Act of २०१४

सूचना प्रविधि तथा साइबर सुरक्षाको क्षेत्रमा अमेरिकी कांग्रेसले यो कानून सन् २०१४ को डिसेम्बर महिनामा

लागु गरेको थियो । संघीय सूचना प्रविधि प्रणाली (Federal Information Technology System) र पूर्वाधार (Infrastructure) लाई व्यवस्थित गर्ने हेतुले यो ऐन जारी गरिएको हो । यस ऐनद्वारा विभिन्न संघीय निकायहरू IT Investment को नियन्त्रणभित्र राखेको पाइन्छ भने संघीय तहमा रहेका Data Center हरूको सूची (Inventory) लगायत Data Center स्थापना गरेको छ ।

(छ) Consumer Privacy Protection Act of २०१७

यो ऐन अमेरिकाको साइबर सुरक्षा र उपभोक्ताहरूको गोपनीयता अलावा अनलाइन उपभोक्ताहरूको गोपनीयता संरक्षणको दृष्टिकोणबाट समेत अत्यन्तै महत्त्वपूर्ण मानिन्छ । यस ऐनले उपभोक्ताहरूको बैयक्तिक डाटा लिई सेवा प्रदान गर्ने संस्थाहरूले गोपनीयता तथा Data Privacy सँग सम्बन्धित केही आधारभूत मापदण्डहरू पालना गर्नका लागि बाध्यकारी हुनुपर्दछ । यस ऐनले उपभोक्ताका विभिन्न प्रकारका Data हरूको सुरक्षाका सन्दर्भमा व्यवस्था गरेको छ । ती यस प्रकार छन् ।

- Social Security Number र सरकारले प्रदान गरेका अन्य Identification Numbers,
- वित्त तथा आर्थिक कारोबारसँग सरोकार राख्ने खाता तथा क्रेडिट कार्ड नम्बरहरू,
- ईमेल ठेगाना र पासवर्डलगायत अन्य अनलाइनका यूजर नेम र पासवर्डहरू,
- Finger Print, Face recognition र अन्य बायोमेट्रिक डाटाहरू,
- उपभोक्तामा भौतिक तथा मानसिक स्वास्थ्यसँग सम्बन्धित डाटाहरू,
- Geo-location सँग सम्बन्धित डाटाहरू,
- व्यक्तिगत डिजिटल फोटो तथा भिडियोहरूको पहुँच ।

२.३.३. संयुक्त अधिराज्य

संयुक्त अधिराज्यमा साइवर कसूरको नियन्त्रणको लागि Obscene Publications Act, १९५९, Forgery and Counterfeiting Act, १९८१, Police and Criminal Evidence Act, १९८४, Computer Misuse Act, १९९०, Data Protection Act, १९९८, Regulation of Investigatory Power Act, २००० लगायतका कानूनहरू कार्यान्वयनमा रहेका छन् । [१६]

२.३.४. दक्षिण कोरिया

दक्षिण कोरियामा साइबर सुरक्षा सम्बन्धी कानूनको आवश्यकता सम्बन्धमा सन् १९८० देखि नै कुरा चली सन् १९८६ मा " Expansion and Promotion of Utilization of Communications Network Act" को तर्जुमा भई सोही ऐनद्वारा डाटाको सुरक्षा सम्बन्धी कानूनी व्यवस्था गरेको पाइन्छ । सन् २००१ मा दक्षिण कोरियाले पहिलोपल्ट राष्ट्रियव्यापी साइबर संकटको सामना गरे पश्चात साइबर सुरक्षालाई राष्ट्रिय सुरक्षाको एक स्तम्ब मानी दक्षिण कोरियाली सरकारले यस विषयसँग सम्बन्धित विभिन्न नीति, कानून तथा रणनीतिहरुको तर्जुमा गरेको देखिन्छ । सन् २००१ मा नै " Communication Infrastructure Protection Act, २००१"को तर्जुमा गरी कम्प्युटरको दुरुपयोगलाई

१६ https://securelist.com/cybercrime-and-the-law-a-review-of-uk-computer-crime-legislation/३६२५३/ (Assessed on February ९, २०२४)

अपराधिकरण गरिएको थियो भने "Promotion of Utilization of Information and Communications Network Act"लाई संशोधन गरी "Promotion of Utilization of Information and Communications Network and Data Protection Act"नामाकरण गरी डाटा सुरक्षा सम्बन्धी थप प्रावधानहरु समावेश गरिएको थियो।[१७]

हाल साइबर सुरक्षा सम्बन्धमा दक्षिण कोरियामा एकीकृत ऐन नभए तापनि विभिन्न ऐनहरुमा यस विषयसँग सम्बन्धित प्रावधानहरु व्यवस्था गरेको पाइन्छ। साइबर सुरक्षा सम्बन्धमा मुख्य गरी "Protection of the Information and Communications Infrastructure Act, २००१ (amended २०१३) र "Personal Information Protection Act, २०११(amended २०२०) ले व्यवस्था गरेको छ। यस ऐनको (Protection of the Information and Communications Infrastructure Act, २००१ (amended २०१३) मुख्य उद्देश्य कृर्टिकल सूचना र सञ्चार पूर्वाधारहरुको (Critical information and communication infrastructure) संरक्षण सम्बन्धी उपायहरूको तर्जुमा र कार्यान्वयन गरी त्यस्ता पूर्वाधारहरुलाई विद्युतीय माध्यमबाट हुने घुसपेठ(electronic intrusion) बाट जोगाई स्थिर रूपमा सञ्चालन गर्नु रहेको छ[१८] .

Personal Information Protection Act, २०११ ले सरकारी र निजी निकायहरूद्वारा व्यक्तिगत डाटाको सङ्कलन, प्रयोग, खुलासा र अन्य प्रशोधनलाई नियमित गर्ने सम्बन्धमा व्यवस्था गरेको छ।[१९] PIPA ले व्यक्तिगत डाटा सुरक्षामा सामान्य कानूनको रूपमा कार्य गर्दछ जुन साइबर आक्रमण र डाटा चुहावट सहित डाटा गोपनीयता उल्लङ्घनका सबै घटनाहरूमा नेटवर्क ऐनसँग संयोजनमा लागू हुन्छ। साथै

दक्षिण कोरियामा Electronic Financial Transaction Act,२००६ समेत तर्जुमा भई प्रचलनमा रहेको छ जस अन्तर्गत वित्तीय कम्पनीहरूको नेटवर्क प्रणालीहरूमा इलेक्ट्रोनिक घुसपैठ (electronic intrusion) लाई निषेधित गरिएको छ। [२०] सो ऐनहरु बाहेक क्रेडिट सूचना प्रयोग र संरक्षण ऐन (The Credit Information Use and Protection Act, २००९) समेत प्रयोगमा रहेको छ जसले क्रेडिट जानकारी सङ्कलन, प्रयोग, अनुसन्धान, व्यवस्थापन वा उपलब्ध गराउने संस्थाहरू ('क्रेडिट सूचना कम्पनीहरू') लाई नियमन गर्छ र त्यस्ता संस्थाहरूलाई क्रेडिट जानकारी कम्प्यूटर प्रणालीको संरक्षण गर्नका लागि प्राविधिक, भौतिक र प्रशासनिक सुरक्षा उपायहरू प्रयोग

---

१७ https://www.kdevelopedia.org/Resources/view/०४२०१७०१२४०१४७१०३.do, accessed on २८ March, २०२४.

१८ Protection of the Information and Communications Infrastructure Act, २००१, Article १-The purpose of this Act is to operate critical information and communications infrastructure in a stable manner by formulating and implementing measures concerning the protection of such infrastructure, in preparation for intrusion by electronic means, thereby contributing to the safety of the nation and the stability of the life of people.

Article २- (Definitions)- १.The term "information and communications infrastructure" means electronic control and management system related to the national security, administration, defense, public security, finance, communications, transportation, energy, etc. and information and communications network under Article २ (१) १ of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.;

(२) The term "electronic intrusions" means acts of attacking information and communications infrastructure by hacking, computer viruses, logic or email bombs, denial of service, or high power electromagnetic waves, etc.; Available at-https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=२८८१२&type=part&key=४३, accessed on २८ March, २०२४.

१९ Available at- https://www.dataguidance.com/legal-research/personal-information-protection-act-२०११-०, accessed on २८ March, २०२४.

२० Available at- https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=४४४५५&type=part&key=८, accessed on २८ March, २०२४.

गर्न बाध्यकारी गराउँछ ।

No legislation in South Korea specifically addresses cybersecurity, but several data protection laws and regulations in South Korea contain provisions related to cybersecurity.

The main laws and regulations related to data protection and cybersecurity are the Personal Information Protection Act २०११ (as amended in २०२०) ('PIPA') and its implementing regulations, which regulate the collection, use, disclosure, and other processing of personal data by governmental and private entities. Among the PIPA's implementing regulations is the Standards of Personal Information Security Measures (only available in Korean here) ('the Standards') which prescribe detailed security measures for personal data processing systems.

Following recent amendments to data protection laws and regulations in South Korea that went into effect on ५ August २०२० ('the २०२० Amendments'), most of the provisions related to the processing of personal data, including those that specifically apply to an information and communications service providers ('ICSPs'), have been transferred to the PIPA.

In addition, ICSPs are required, under the Act on Promotion of Information and Communication Network Utilization and Information Protection २००१ (as amended) (up-to-date version only available in Korean here) ('ICNA'), to implement security measures to ensure the safety of networks and the reliability of data used for the provision of information and communications services, and are further recommended (though not legally required) to follow the Guidance on Data Protection Measures (only available to download in Korean here). In addition, the Standards of Technical and Managerial Security Measures (only available in Korean here) ('the ICSP Standards'), an implementing regulation of the ICNA, prescribe detailed security measures for ICSPs' data processing systems (similar to those prescribed by the Standards).

Although the PIPA will mainly apply to the processing of personal data by ICSPs, special provisions of the ICNA may apply ahead of the PIPA in certain cases.

Concerning cloud computing, the Act on the Development of Cloud Computing and Protection of its Users २०१५ (up-to-date version only available in Korean here) ('the Cloud Computing Act') and the Standards of Data Protection for Cloud Computing Services (only available in Korean here) ('Cloud Computing Standards') apply. The Cloud Computing Standards are an implementing regulation of the Cloud Computing Act, which recommend, though not legally require, security measures for cloud computing. Also, under recent amendments to the Cloud Computing Act (only available in Korean here) scheduled to go into effect on १२ January २०२३, the Ministry of Science and ICT ('MSIT') will be permitted to provide security

certification for cloud computing services that comply with the Cloud Computing Standards.

The Act on the Protection of Information and Communications Infrastructure २००१ (up-to-date version only available in Korean here) ('the Infrastructure Act') contains requirements for the protection of critical information and communications infrastructure.

Finally, for financial institutions or enterprises processing personal credit information, additional cybersecurity provisions can be found in several other sectoral laws and regulations, such as the Use and Protection of Credit Information Act १९९५ (up-to-date version only available in Korean here) ('CIUPA'), the Electronic Financial Transactions Act २००६ ('EFTA'), and the Regulation on the Supervision of Electronic Financial Transactions (only available in Korean here) ('the EFTA Regulation'). All of the laws above and regulations are currently in force.

२.३.५. सिंगापुर

(१) Intercom Security Master Plan (ISMP: २००५-२००७)

सिंगापुरको Ministry of Communication and Information (MCI) अन्तर्गत स्थापना भएको "The Info-Communications Development Authority (IDA) ले पहिलो पटक सिंगापुरमा साइबर सुरक्षाको क्षेत्रमा गुरु योजना (Master Plan) तयार गरेको थियो जसले सिंगापुरको सरकारी कार्यालयहरूमा साइबर सुरक्षाको क्षेत्रमा गरिएका प्रयासहरूलाई संयोजन गर्ने प्रमुख भूमिका निभाउँदै साइबर सुरक्षाका लागि सरकारी तवरबाट गरिनुपर्ने कार्यहरूको मापदण्ड तयार पारेको थियो । यसको मुख्य उद्देश्य सिंगापुरको सरकारी क्षेत्रमा साइबर सुरक्षाको क्षेत्रमा कार्य गर्नु र साइबर कसूरहरूलाई निस्तेज पार्नका लागि आवश्यक प्राविधिक जनशक्तिहरूको परिचालन गर्नु थियो । ४९ त्यस्तै यो योजनाको निरन्तरताको लागि यो योजनाको समाप्तिपश्चात् सिंगापुरले दोस्रो बृहत् योजनाको रूपमा The Infocomm Security Master Plan (२००८-२०१२) तर्जुमा गरी कार्यान्वयनमा ल्याएको थियो । जसको मुख्य परिलक्ष्य "Making Singapore a Security and Trusted Hub" थियो । यो योजनाले मूलतः सिंगापुरको Critical Infocomm Infrastructure (CII) लाई सुदृढीकरण गर्ने मुख्य योजना लिएको थियो ।

(२) Personal Data Protection Act, २०१२

व्यक्तिगत डाटा सुरक्षा एउटा फरक विधा भए तापनि यो साइबर सुरक्षासँग प्रत्यक्ष सरोकार राख्ने विषय हो । यहाँ सबैभन्दा प्राथमिकताको विषय व्यक्तिगत डाटा हुने हुनाले र साइबर सुरक्षाको पाटोबाट हेर्दा पनि योसँग सम्बन्धित कानून कानूनी रूपमा व्यक्तिसँग सम्बन्धित डाटाहरूको व्यवस्थापन, प्रयोग र सुरक्षाको मापदण्डका विषयहरूमा जोड दिन्छ ।

(३) National Cyber Security Master Plan (NCSM), २०१८

यो योजना सिंगापुरको सबैभन्दा पछिल्लो साइबर सुरक्षाको सम्बन्धमा बनेको बृहत् योजना हो । जसले सिंगापुरका आम सूचना प्रविधि प्रयोगकर्ता तथा इन्टरनेट प्रयोगकर्ताहरूको साइबर सुरक्षाका पक्षहरूलाई समेत समेटेको

पाइन्छ । यो गुरु योजना (Master Plan) को आधारका रूपमा यस अगाडिका दुईवटा गुरु योजना (Master Plan) हरूलाई लिइएको पाइन्छ तर यसको क्षेत्र अधिल्ला दुईवटा योजनाको भन्दा व्यापक बनाइएको छ । यसले सिंगापुरको साइबर सुरक्षाको क्षेत्रलाई थप परिपक्क, सम्बृद्ध बनाई थप उचाई प्रदान गरेको पाइन्छ । सन् २००५ को योजनाले समेटेको सरकारी तहको साइबर सुरक्षा सन् २००८ को योजनाले समेटेको Critical Infocomm Infrastructure का अलावा यस गुरु योजना (Master Plan) ले आफ्नो क्षेत्रलाई थप फराकिलो बनाउँदै सूचना प्रविधिलाई प्रयोग गर्ने सम्पूर्ण व्यापारका क्षेत्रहरूलगायतका व्यक्तिगत साइबर सुरक्षालाई पनि उत्तिकै महत्त्वपूर्ण स्थान दिएको पाइन्छ ।

(४) Computer Misuse and Cyber Security Act,२०१८

सिंगापुरको साइबर कसूरको क्षेत्रमा जारी गरिएको आधारभूत कानूनको रूपमा The Computer Misuse Act (CMA) को जुन सन् १९९३ मा जारी गरिएको थियो र यसले साइवर कसूरसँग सम्बन्धित विषयलाई सम्बोधन गरेको थियो । सिंगापुरमा विभिन्न समयमा भएका साइवर हमलाहरूको कारण यस्ता गतिविधिहरूलाई रोक्न यस ऐनलाई सन् २००७ मा Computer misuse and Security Act (CMCS), २००७ ले प्रतिस्थापन गरेको थियो । यसलाई सिंगापुरको सन् २०१३ मा ल्याएको National Cyber Security Master Plan (NCSMP), २०१८ का आधारमा परिवर्तन गरिएको थियो ।

सिंगापुरमा साइबर सुरक्षा सम्बन्धमा मुख्य रुपमा साइबर सुरक्षा ऐन, २०१८ (Cyber Security Act,२०१८) ले कानूनी व्यवस्था गरेको पाइन्छ । साइबर सुरक्षा खतराहरू र घटनाहरूलाई रोक्न, व्यवस्थापन गर्न र प्रतिक्रिया दिन, महत्त्वपूर्ण सूचना पूर्वाधारका स्वामित्व भएकाहरूलाई नियमन गर्न, साइबर सुरक्षा सेवा प्रदायकहरूलाई नियमन गर्न, र यससँग सम्बन्धित मामिलाहरू नियमन गर्ने प्रयोजनार्थ साइबर सुरक्षा ऐन, २०१८ तर्जुमा भएको देखिन्छ ।[२१] यस ऐनले दफा २ मा साइबर सुरक्षाको परिभाषा निम्न बमोजिम गरेको छ-

" the state in which a computer or computer system is protected from unauthorized access or attack, and because of that state-

- The computer or computer system continues to be available and operational;
- The integrity of the computer or computer system is maintained; and
- The integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained."

यस ऐनको चार वटा मुख्य उद्देश्यहरू रहेका छन्, जुन देहाय बमोजिमका रहेका छन्:

- साइबर हमलाहरू विरुद्ध कृर्टिकल सूचना पूर्वाधारहरुको (Critical information infrastructure) को सुरक्षा बलियो बनाउने,

---

२१ Cyber security Act, २०१८, Preamble- "An Act to require or authorize the taking of measures to prevent, manage, and respond to cyber security threats and incidents, to regulate owners of critical information infrastructure, to regulate cyber security service providers, and for matters related thereto, and to make consequential or related amendments to certain other written laws. Available at- https://sso.agc.gov.sg/Acts-Supp/९-२०१८/, accessed on २७ March, २०२४.

- साइबर सुरक्षाका खतराहरू र घटनाहरूलाई रोक्न र प्रतिक्रिया दिन सिंगापुरको साइबर सुरक्षा एजेन्सी (Cyber Security Agency) लाई अधिकार दिने,
- साइबर सुरक्षा सम्बन्धी जानकारी दिनका लागि साझा संरचना स्थापना गर्ने,
- साइबर सुरक्षा सेवा प्रदायकहरूको लागि इजाजतपत्र ढाँचा स्थापना गर्ने,

सो ऐनले कृर्टिकल सूचना पूर्वाधारको रुपमा अत्यावश्यक सेवाको निरन्तर वितरणको लागि आवश्यक हुने कम्प्युटर वा कम्प्युटर प्रणालीलाई मानेको छ जसमा हानी भएमा सिंगापुरमा आवश्यक सेवाको उपलब्धतामा नै नकरात्मक प्रभाव पार्दछ।

साइबर सुरक्षा ऐन, २०१८ बाहेक सिंगापुरमा अनाधिकृत पहुँच वा परिमार्जन विरुद्ध कम्प्युटर सामग्री सुरक्षित गर्न, राष्ट्रिय डिजिटल पहिचान सेवाको दुरुपयोग रोक्न र यससँग सम्बन्धित मामिलाहरूको लागि व्यवस्था गर्न Computer Misuse Act, १९९३(Revised २०२०) तर्जुमा भई प्रचलनमा रहेको देखिन्छ।[२२] यस ऐनले परिच्छेद २ मा दफा ३ देखि १२ सम्म विभिन्न कार्यलाई अपराधिकरण गरेको छ जुन निम्न बमोजिमको रहेको छ।

Section	Offence
३	Unauthorized access to Computer material
४	Access with intent to commit or facilitate commission of offence
५	Unauthorized modification of computer material
६	Unauthorized use or interception of computer service
७	Unauthorized obstruction of use of computer
८	Unauthorized disclosure of access code
८A	Disclosure of password, access code, etc., in relation to national digital identity service
८B	Supplying, etc., credential of another person
९	Supplying, etc., personal information obtained in contravention of certain provisions
१०	Obtaining, etc., items for use in certain offences
११	Enhanced punishment for offences involving protected computers
१२	Abetments and attempts punishable as offences

सन् २०१२ मा सिंगापुरमा आधारभूत डाटा संरक्षण कानूनको रूपमा Personal Data Protection Act (PDPA) लागू गरिएको थियो जसमा व्यक्तिगत डाटाको सङ्कलन, प्रयोग, खुलासा र संरक्षण सम्बन्धमा व्यवस्था गरिएको छ। सन् २०२० मा PDPA लाई मा संशोधन गरी उपभोक्ताको डाटा संरक्षण सम्बन्धी कानूनी प्रावधानहरुलाई समावेश

२२ Computer Misuse Act, १९९३-An Act to make provision for securing computer material against unauthorized access or modification, for preventing abuse of the national digital identity service, and for matters related thereto. Available at- https://sso.agc.gov.sg/Act/CMA१९९३?ProvIds=al-#al-, accessed on २७ March, २०२४.

गरिएको थियो । यस ऐनले व्यक्तिहरूको व्यक्तिगत डाटाको सुरक्षा गर्न पाउने अधिकारका साथै वैध र व्यावहारिक उद्देश्यका लागि त्यस्ता डाटा सङ्कलन, प्रयोग वा खुलासा गर्नपर्ने संस्थाहरूको आवश्यकता दुबैलाई मान्यता दिन्छ ।

२.४ साइबर कसूर सम्बन्धी अन्तराष्ट्रिय महासन्धी (International Convention)

२.४.१ साइबर कसूरसम्बन्धी बुढापेष्ट महासन्धि

युरोपियन परिषद्को साइबर कसूरसम्बन्धी महासन्धि' बेल्जियमको बुढापेष्टमा २३ नोभेम्बर, २००१ ई.सं. देखि सबै राष्ट्रहरूका लागि हस्ताक्षर खुला गरिएको हो । दक्षिण एसियाली एक मात्र मुलुक श्रीलङ्कालगायत ५५ राष्ट्रहरू यस महासन्धिका पक्ष राष्ट्रहरू रहेका छन् । साइबर कसूर नियन्त्रणका लागि यस महासन्धिले निम्न तीन क्षेत्रमा बाध्यात्मक कानूनी संरचनाको आधार निर्माण गरेको छ ।

१. **सारवान पक्ष:** साइबर स्पेस तथा कम्प्युटर प्रणालीको उचित प्रयोग तथा निष्ठालाई कायम राख्न सोविरुद्धका निम्न कार्यहरूलाई महासन्धिले कसूरजन्य कार्यको रूपमा परिभाषित गरेको छ ।

(क) अनधिकृत प्रवेश:

मनसायपूर्वक बिनाअधिकार कम्प्युटर प्रणालीमा प्रवेश गर्नु, जसलाई ह्याकिङ पनि भनिन्छ । यसरी पूरै कम्प्युटर प्रणाली वा सोको कुनै भागमा मात्र प्रवेश गर्नुलाई पनि कसूरजन्य कार्य मानिएको छ । यस्तो कार्य सुरक्षा संयन्त्रलाई तोडेर कम्प्युटर डाटा प्राप्त गर्न वा अन्य बदनियत राखी वा एउटा कम्प्युटर प्रणालीबाट अर्को प्रणालीका सम्बन्धमा पनि हुन सक्छ ।

(ख) अनधिकृत अन्तरग्रहण:

सार्वजनिक रूपबाट प्रसारण नभएका वा व्यक्तिगतरूपमा प्रसारण भएका डाटाहरूलाई मनसायपूर्वक बिनाअधिकार कुनै प्राविधिक माध्यमबाट प्राप्त गर्ने वा हस्तक्षेप गर्ने कार्यलाई कसूरजन्य मानिएको छ । यो कार्य प्रणालीलाई बाह्य हस्तक्षेप गरेर वा कम्प्युटर प्रणालीबाट वा सोही प्रणालीभित्रबाट जसरी पनि भएको हुन सक्छ । यसअन्तर्गत अन्य व्यक्तिहरूको वार्ता रेकर्ड गर्नु, सुन्नु, अनुगमन वा निगरानी गर्नु जस्ता कार्यहरूलाई समेत समेटिएको छ ।

(ग) डाटामा हस्तक्षेप:

बिनाअधिकार मनसायपूर्वक अरूको कम्प्युटर डाटालाई नोक्सान पु¥याउनु, मेटनु, गुणस्तरमा ह्रास गराउनु, बदल्नुवा दबाउनुजस्ता कार्यहरूलाई पनि कसूरजन्य कार्य मानिएको छ ।

(घ) प्रणालीमा हस्तक्षेप:

कम्प्युटर प्रणालीको गतिविधिमा गम्भीर बाधा पु¥याउने कार्य । यस्तो कार्य कम्प्युटर प्रणालीमा केही कुरा प्रवेश गराई वा प्रसारण गरी वा नोक्सान पु¥याई, मेटाई, स्तरह्रास गरी वा बदली वा दबाएर जुनसकै तवरबाट अनधिकृतरूपले मनसायपूर्वक भएकोमा कसूरजन्य मानिएको छ ।

(ङ) यन्त्रको दुरूपयोग:

साइबर कसूरजन्य कार्यमा प्रयोग हुने गरी लक्षित र निर्माण गरिएका कुनै पनि संयन्त्रहरूको अनधिकृत तवरले उत्पादन, आयात–निर्यात, खरिद–बिक्री तथा वितरण जस्ता कार्यहरू, जसमा त्यस्ता कसूरजन्य कार्यहरूमा प्रयोग हुने कम्प्युटर प्रोग्राम, कम्प्युटर पासवर्ड, प्रवेश कोडसमेतलाई समेटिएको छ। कसूर गर्ने मनसायले त्यस्ता संयन्त्रहरू राख्नुलाई पनि कसूर मानिएको छ।

(च) कम्प्युटरसम्बद्ध कसूरहरू:

यसअन्तर्गत पराम्परागत कसूरहरूलाई समेटिएका छन् । अर्थात् कम्प्युटर प्रणालीको दुरूपयोगबाट गरिने परम्परागत कसूरहरूलाई समेत कसूरजन्य कार्यको रूपमा महासन्धिले समेटेको छ, जो निम्न प्रकार रहेको छ।

- धोखाधडी वा ठगी र किर्ते जालसाजी
- बालबालिकासम्बन्धी अश्लील सामग्रीः बालबालिका जस्तो देखिने अवास्तविक (काल्पनिक) तस्बिरहरू र बालबालिकासम्बन्धी अश्लील सामग्रीहरूको उत्पादन र वितरण मात्र होइन, सङ्ग्रह वा राख्ने कार्यसमेतलाई कसूरजन्य कार्यको रूपमा समेटिएको छ।
- बौद्धिक अधिकारको संरक्षण: यो महासन्धिले बौद्धिक सम्पत्तिविरूद्धको कसूरका बारेमा छुट्टै नियमहरूको निर्माण गरेको छैन तथापि बौद्धिक सम्पत्तिको संरक्षणका विषयमा कम्प्युटर प्रणालीको दुरूपयोगबाट सोको विद्यमान नियम कानूनहरूको उल्लङघन भएकोमा सोहीबमोजिम कारबाही र सजाय हुनुपर्ने कुरालाई प्रत्याभूत गरेको पाइन्छ।

२. कार्यविधिगत पक्ष

आधिकारिक तवरबाट प्रमाणको संरक्षण, सङ्कलन तथा सूचना आदान–प्रदान गर्न महासन्धिले अत्यन्त महत्वपूर्ण एवं विस्तृत कार्यविधिगत नियमहरू प्रतिपादन गरेको छ। कम्प्युटर प्रणालीसँग सम्बन्धित डाटाहरूको प्रकृतिबमोजिम तुरुन्त हराउन सक्ने, गतिशील रहने, निश्चित समय चक्रसम्म संरक्षित रहने वा भण्डारण भइरहने आदि विविध प्रकारका हुन्छन् । यद्यपि यस्ता डिजिटल प्रविधिका प्रमाणहरू तुरुन्त मेटाउन सकिने, सम्पादन गर्न सकिने, एक रूपबाट अर्को रूपमा बदल्न सकिने र स्तानान्तरण गर्न सकिने खालका हुने भएकाले अत्यत्त संवेदनशील हुन्छन्। अतः यथासमयमा सो प्रमाणहरूको संरक्षण हुनु अति जरुरी हुन्छ। यसका लागि महासन्धिले सेवा प्रदायकहरूलाई विशेष जिम्मेवारी तोकेको छ । अधिकारप्राप्त निकाय वा अधिकारीले कानूनबमोजिम जारी गरेको आदेशको आधारमा प्रमाणहरूको संरक्षण, आवश्यक सूचनाहरूको उपलब्धता, खानतलासी तथा बरामदी हुन सक्ने गरी सदस्य राष्ट्रहरूका लागि एक रूपको नियम तथा मापदण्ड तय गर्नमा जोड दिएको देखिन्छ । साथै, व्यक्तिका गोपनीयताको हकको सम्मान, मानवअधिकार संरक्षणसम्बन्धी दस्तावेजहरूको परिपालना, कार्यविधिगत पक्षको अस्मिता र विश्वसनीयताको प्रत्याभूति गर्न निश्चित मापदण्ड तथा बाध्यकारी नियमहरूको व्यवस्था गरिएको पाइन्छ । सो कार्यविधिगत नियमहरूको प्रयोग र लागू हुने सीमा यस प्रकार तोकिएको छ–

- महासन्धिले कसूरजन्य घोषणा गरेका कार्यहरूको अनुसन्धान।
- कम्प्युटर प्रणालीको माध्यमबाट गरिएका कुनै पनि कसूरको अनुसन्धान।

- कुनै पनि अनुसन्धानका लागि आवश्यक डिजिटल प्रविधिमा राखिएका प्रमाणहरूको सङ्कलन।

३. अन्तर्राष्ट्रिय सहयोग

साइबर कसूर बहुक्षेत्रीय प्रकृतिको रहेको हुनाले यसमा प्रयोग हुने सारवान कानून तथा क्षेत्राधिकारको विषय निसन्देह जटिल छ। परम्परागत क्षेत्राधिकारको अवधारणाले यस्ता कसूरहरूको अनुसन्धानको पाटोलाई सीमित गर्दछ भने कम्प्युटर डाटा भण्डारण हुने क्षेत्र (ऋयिगम) को स्थान पहिचान गर्न अझै जटिल रहेको छ। अतः इन्टरनेटको विश्वव्यापी आयाम तथा साइबर कसूरको अन्तर्राट्रिय स्वरूपलाई पहिचान गर्दै यस विषयमा अन्तर्राष्ट्रिय समुदायको आपसी सहयोगको क्षेत्रलाई व्यवहारिक तथा कार्यात्मक ढङ्गबाट मूर्त रूप दिने कार्यमा महासन्धिको विशेष महत्व रहेको छ।

अन्तर्राष्ट्रिय सहयोगका लागि सर्वप्रथम साइबर कसूरसम्बन्धी सर्वस्वीकार्य न्यूनतम मापदण्डहरूको निर्धारण गरिएको छ र आवश्यकता अनुसार अन्तर्राष्ट्रिय सहयोगका स्पष्ट मार्ग तथा कार्यविधिहरूको नौलो र विशिष्ट प्रावधानहरूको व्यवस्था गरिएका छन्। जसमा कम्प्युटर प्रणालीसम्बन्धी महत्वपूर्ण सूचनाहरूको स्वतःस्फूर्त आदन–प्रदान, डाटाहरूको उचित संरक्षण, कम्प्युटर डाटामा आधिकारिक प्रवेश तथा प्राप्तिका लागि आपसी सहयोगका साथै त्यस्ता सहयोग र समन्वयलाई प्रभावकारी बनाउने जुनसुकै समयमा निर्वाधरूपले निरन्तर सम्पर्क गर्न सकिने ७–२४ सम्पर्क सञ्जालको व्यवस्था तथा तत्सम्बन्धी स्पष्ट कार्यविधिहरू विशेष महत्वको रहेको देखिन्छ। ७–२४ सम्पर्क सञ्जाल केन्द्रबिन्दुको स्थापना सबै सदस्य राष्ट्रका लागि बाध्यात्मक रहनुका साथै अन्तर्राष्ट्रिय सहायताको सहजीकरणका लागि सो केन्द्रबाट निम्न कार्यहरू गर्ने व्यवस्था रहेको छ–

- प्राविधिक सहयोग र सल्लाह आदान–प्रदान गर्ने।
- कम्प्युटर डाटाको वैधानिक तथा उचित संरक्षणका लागि उपयुक्त संयन्त्रहरूलाई क्रियाशील राख्ने।
- प्रमाणहरूको तत्काल सङ्कलन गर्ने।
- शङ्कास्पद गतिविधिहरूको पहिचान गर्ने र पत्ता लगाउने।

महासन्धिको योगदान र उपयोगिता विश्वव्यापी परिघटनाको रूपमा रहेको साइबर स्पेस तथा कम्प्युटर प्रणालीको उपयोगिता तथा अस्मितालाई कायम राक्नमा प्रतिबद्ध यस साइबर कसूरसम्बन्धी महासन्धिको योगदान र उपयोगितालाई बुँदागतरूपमा निम्नबमोजिम उल्लेख गर्न सकिन्छ।

साइबर कसूरसम्बन्धी कानूनको विकास तथा सामञ्यस्यतामा यस महासन्धिको विश्वव्यापी प्रभाव रहेको छ। साइबर कसूरसम्बन्धी फौजदारी न्याय प्रणालीको आधारभूत मापदण्ड तय गरी विभिन्न कानून प्रणालीहरूबीच एकरूपता तथा सामञ्जस्यता कायम गर्नमा भूमिका रहेको छ। पक्ष राष्ट्रहरूबीच आपसी विश्वास र सहयोग बढाएको छ। क्षमता अभिवृद्धिमा अभियन्ताको भूमिका निर्वाह गरेको छ। कानूनी सुनिश्चितता प्रदान हुनुका साथै निजी क्षेत्रको विश्वास आर्जन गरेको छ। साइबर स्पेसको उचित प्रयोगका लागि आवश्यक नीति तथा नियमहरूको निर्माण गरेको छ। साइबर स्पेसको प्रयोगमा मानवअधिकार तथा कानूनी शासनलाई प्रवद्र्धन गरेको छ। प्रत्येक व्यक्ति तथा व्यक्तिगत अधिकारको सुरक्षामा प्रतिबद्ध रहेको छ।

परिच्छेद तीन

पूर्व अध्ययन कार्यको पुनरावलोकन तथा समिक्षा

३.१ पूर्व अध्ययन कार्यको पुनरावलोकन तथा समिक्षा (Review of the Literature)

प्रस्तुत अध्ययनको क्रममा यस विषयसँग सम्बन्धित देहायका सन्दर्भ सामग्रीहरुको अध्ययन तथा पुनरावलोकन गरियोः

१. **साइबर कसूर र हाम्रो न्यायिक अभ्यास: एक विश्लेषण, नेपाल न्यायिक प्रतिष्ठान, रत्नबहादुर वागचन्दः**
नेपालमा साइबर कसूरका विरुद्ध न्यायिक प्रणालीले समाना गरेका प्रमुख समस्याहरूको विस्तृत विश्लेषण प्रस्तुत गरेको छ। यस लेखमा लेखकले न्यायिक प्रक्रियामा साइबर कसूरको जटिलतासँग कसरी जुध्नुपरेको छ, र यससँग सम्बन्धित कानूनी कार्यान्वयन र प्रक्रियागत खामिहरूको विश्लेषण गरेका छन्। लेखकले न्यायाधीशहरूको अनुभव र अदालतमा देखिएका व्यवहारिक समस्याहरूलाई उजागर गर्दै, न्यायिक प्रक्रिया सुधारका लागि आवश्यक सुझावहरू प्रदान गरेका छन्।

लेखमा वर्णन गरिएको छ कि कसरी नेपालमा साइबर कसूरको तीव्र वृद्धिसँगै न्यायिक प्रणालीमा ठूला चुनौतीहरू आउन थालेका छन्। यसले न्यायाधीशहरू, वकिलहरू, र अन्य कानूनी पेशाकर्मीहरूले सामना गर्ने विशेष समस्या र अड्चनहरूको गहिरो अध्ययन गर्दछ। लेखकले अदालतमा साइबर कसूरसम्बन्धी मुद्दाहरूको विचार गर्दा भएका अवरोधहरू र कानूनी प्रक्रिया सुधारका सम्भावित उपायहरूको चर्चा गरेका छन्। यस अध्ययनले न्यायिक अभ्यासको वर्तमान अवस्थालाई राम्रोसँग बुझ्न र न्यायिक सुधारका दिशामा मार्गनिर्देशन गर्नका लागि महत्त्वपूर्ण अन्तर्दृष्टि प्रदान गर्दछ।

साथै, लेखले साइबर कसूरका विषयमा न्यायिक प्रक्रिया र कानूनी ढाँचामा सुधारका लागि आवश्यक कदमहरू पनि प्रस्तुत गरेको छ। यसले न्यायाधीशहरूको दृष्टिकोणलाई समेट्दै, अदालतको कामकाजमा सुधार ल्याउने सम्भावनाहरूलाई विश्लेषण गर्छ। लेखकले व्यावहारिक सुझावहरूको माध्यमबाट न्यायिक प्रणालीलाई अझ प्रभावकारी बनाउनका लागि दिशा निर्देश गरेका छन्, जसले साइबर कसूरको मुद्दामा न्याय प्राप्तिमा सहयोग पुर्‍याउँछ।

समग्रमा, वागचन्दको लेखले नेपालमा साइबर कसूरसम्बन्धी न्यायिक प्रक्रियाको प्रभावकारिता र समस्या क्षेत्रको गहिरो विश्लेषण प्रस्तुत गर्दै, कानूनी सुधारका लागि व्यावहारिक सुझावहरू प्रदान गरेको छ। यस अध्ययनले न्यायिक ढाँचामा सुधारका लागि आवश्यकीय दिशा निर्धारणमा मद्दत पुर्‍याउँछ र साइबर कसूरका मुद्दाहरूलाई प्रभावकारी ढंगले व्यवस्थापन गर्नका लागि आवश्यक कदमहरूको चर्चा गर्छ।

२. **नेपाल ल क्याम्पसबाट प्रकासित नेपाल कानून परिचर्चा जर्नलमा समाबेश किशोर सापकोटाले लेख्नु भएको साइबर सुरक्षा, साइबर कसूर र साइबर कानूनको बुझाइ र यथार्थ :**
नेपालमा साइबर कानून कार्यान्वयनको एक विवेचनात्मक अध्ययन भन्ने लेखको पुनरावलोकन गरिएको थियो। उपरोक्त लेखह मुलतः नेपालको न्यायिक अभ्यास र कानून कार्यान्वयनको क्रममा देखा परेको समस्याको सम्बन्धमा

मात्र केन्द्रित रहेको छ। यस लेखले नेपालमा साइबर कानूनको कार्यान्वयनमा भएका समस्याहरूको गहिरो विश्लेषण प्रस्तुत गरेको छ। यस लेखमा, लेखकले नेपालमा प्रचलित साइबर कानूनहरूको प्रभावकारिता र कार्यान्वयनमा आएका प्रमुख चुनौतीहरूको अध्ययन गरेका छन्। सापकोटाले कानून र नीतिहरूको वास्तविक यथार्थलाई विश्लेषण गर्दै, नेपालमा साइबर सुरक्षा र कसूरसँग सम्बन्धित समस्याहरूलाई उजागर गरेका छन्। उनले कानूनी कार्यान्वयनमा रहेका खामिहरू, अदालतमा देखिएका समस्याहरू, र सुधारका सम्भावित उपायहरूको चर्चा गर्दै, व्यावहारिक सुझावहरू प्रस्तुत गरेका छन्। यस लेखमा, लेखकले नेपालमा साइबर कानूनको प्रभावकारिता र सुधारका आवश्यकताबारे गहिरो अध्ययन गर्दै, सुधारका उपायहरूको व्यावहारिक सुझाव प्रस्तुत गरेका छन्। लेखले साइबर कसूर र सुरक्षा सम्बन्धी कानूनी र नीतिगत पहलहरूको मूल्याङ्कन गर्दै, प्रभावकारी सुधारका लागि आवश्यक कदमहरूको सुझाव दिएको छ। सापकोटाको अध्ययनले साइबर कानूनको कार्यान्वयनमा रहेका समस्याहरू र चुनौतीहरूको विश्लेषण गर्दै, कानूनी सुधार र नीति विकासमा योगदान पुर्याउँछ। यस लेखले नेपालमा साइबर कानूनको प्रभावकारिता सुधार्नका लागि महत्वपूर्ण दिशानिर्देश प्रदान गर्दछ।

३. A Case Study in Gap and Weaknesses in the Existing Legal Framework of Cyber Law in Nepal, नवराज घिमिरे

प्रस्तुत अध्ययन पत्रले नेपालमा आइबर कसूर सम्बन्धी प्रचलित कानूनहरुको अध्ययन गरी सोको सक्षम र दुर्बल पक्षहरुलाई उजागार गरेको छ। साथै यस अध्ययनले साइबर कसूर सम्बन्धी कानून तथा नीतिहरुको कार्यान्वयन गर्दा के कस्ता कमी तथा चुनौतीहरु रहेका छन् सो पहिचान तथा विश्लेषण गरी सुधारका लागि सुझावहरु पेश गरेको छ। यस लेखले नेपालमा साइबर कसूर नियन्त्रण गर्नका लागि प्रचलित कानूनी ढाँचाको प्रभावकारिता र कमजोरीहरूको विश्लेषण गर्दछ। यस अध्ययनमा, लेखकले नेपालका साइबर कानूनहरूको गहिरो विश्लेषण गर्दै, विद्यमान कानूनी ढाँचामा रहेका कमजोरीहरू र सुधारका आवश्यकता भएको क्षेत्रहरूको पहिचान गरेका छन्। घिमिरेले प्रचलित कानूनी ढाँचाको प्रभावकारिता र कार्यान्वयनमा देखिएका खामिहरूलाई उजागर गर्दै, सुधारका लागि व्यावहारिक सुझावहरू प्रस्तुत गरेका छन्। लेखकले नेपालमा साइबर कसूरको नियन्त्रणमा आएको चुनौतीहरू र समस्याहरूको विश्लेषण गर्दै, कानूनी ढाँचामा सुधारका लागि आवश्यक कदमहरूको प्रस्ताव गरेका छन्। यस अध्ययनले साइबर कसूरसम्बन्धी कानूनी व्यवस्था र त्यसको प्रभावकारिता सुधार्नका लागि मार्गनिर्देशन प्रदान गरेको छ। घिमिरेको लेखले नेपालका कानूनी प्रणालीमा रहेका खामिहरूको विश्लेषण गर्दै, प्रभावकारी सुधारको दिशामा सुझावहरू प्रदान गरेको छ। यस लेखले साइबर कानूनको सुधार र नीति विकासमा महत्वपूर्ण योगदान पुर्याउँछ, र कानूनी ढाँचामा सुधारका लागि व्यावहारिक सुझावहरू प्रस्तुत गर्छ।

४. Cyber Laws and Policies in Nepal-ई. सुजन श्रेष्ठ

यस अध्ययनले अन्तराष्ट्रिय स्तरमा साइबर कसूर तथा साइबर सुरक्षाका सम्बन्धमा के कस्ता दस्ताबेजहरु रहेका छन् सोको चर्चा गर्दै नेपालमा यस विषयसँग सम्बन्धित के कस्ता कानून तथा नीतिहरु रहेका छन् सोको उल्लेख गरिएको छ। साथै संस्थागत रुपमा साइबर सुरक्षा तथा साइबर कसूरका सम्बन्धमा नेपालमा साइबर ब्यूरो, Internet Service Provider's Associations of Nepal (ISPAN), Information Security Response Team Nepal (NPCERT) लगायतका संस्थाहरु यस क्षेत्रमा क्रियाशिल रहेका छन्।

यस लेखले अन्तर्राष्ट्रिय स्तरमा साइबर कसूर र साइबर सुरक्षा सम्बन्धी दस्तावेजहरूको विश्लेषण गर्दै, नेपालमा

यस विषयसँग सम्बन्धित कानूनी र नीतिगत पहलहरूको समीक्षा गरेको छ। यस अध्ययनमा, लेखकले नेपालमा साइबर सुरक्षा र साइबर कसूरसँग सम्बन्धित विभिन्न कानून र नीतिहरूको मूल्याङ्कन गरेका छन्। श्रेष्ठले नेपालमा साइबर सुरक्षा प्रवर्द्धनका लागि क्रियाशील संस्थाहरू, जस्तै साइबर ब्यूरो, ISPAN, र NPCERT का भूमिकाको विश्लेषण गरेका छन्। लेखमा, लेखकले अन्तर्राष्ट्रिय कानूनी मानकसँग नेपालका कानून र नीतिहरूको तुलना गर्दै, संस्थागत पहलहरूको प्रभावकारिता र सुधारका सम्भावित क्षेत्रहरूको चर्चा गरेका छन्। यस लेखले नेपालमा साइबर सुरक्षा र साइबर कसूरको व्यवस्थापनमा सुधारका लागि आवश्यक कानूनी र नीतिगत सुधारको दिशा निर्देश गर्दछ। श्रेष्ठको अध्ययनले नेपालमा साइबर सुरक्षा र कानूनी ढाँचामा सुधारका लागि मार्गदर्शन गर्दै, प्रभावकारी नीतिगत र कानूनी समाधानहरूको प्रस्तुति गरेको छ। समग्रमा, यो लेख नेपालका साइबर कानून र नीतिहरूको मूल्याङ्कन गर्दै, सुधारका दिशामा महत्वपूर्ण सुझावहरू प्रदान गर्दछ।

५. Cyber Crime, Cyber Threat, Cyber Security Strategies and Cyber Law in Nepal, Pramana Research Journal, Vol.९, Issue ३, २०१९, -शैलेन्द्र गिरी

विश्वमा सबैभन्दा छिटो बढ्दो कसूरका रुपमा साइबर कसूर रहेको उल्लेख गर्दै यस अध्ययनले नेपालमा बलियो साइबर सुरक्षा चाहिने विषयलाई जोड दिएको छ। हाल विश्वमा साइबर सुरक्षालाई राष्ट्रिय सुरक्षाको अङ्गका रुपमा लिने गरेको परिप्रेक्ष्यमा नेपालमा पनि यस विषयलाई महत्वपूर्ण मानी आवश्यक कानून तथा नीतिहरुको निर्माण गर्नुपर्ने देखिएको निष्कर्ष यस अध्ययनले निकालेको छ।

यो लेखले साइबर कसूरको वैश्विक वृद्धिलाई र नेपालमा बलियो साइबर सुरक्षा आवश्यकताको महत्वलाई जोड दिएको छ। लेखकले यो अध्ययनमा साइबर सुरक्षा र कसूरलाई राष्ट्रिय सुरक्षा मुद्दाको रूपमा लिइनुपर्ने आवश्यकता बारे चर्चा गर्दै, नेपालमा यस सन्दर्भमा कानूनी र नीतिगत सुधारको आवश्यकता उल्लेख गरेका छन्। लेखमा, गिरीले विश्वव्यापी दृष्टिकोणमा साइबर सुरक्षा र कसूरका रणनीतिहरूको विश्लेषण गर्दै, नेपालमा प्रभावकारी साइबर सुरक्षा रणनीतिहरूको आवश्यकता र सुधारका सुझावहरूको प्रस्तुति गरेका छन्। यस लेखले साइबर सुरक्षा र कसूरको प्रभावकारी व्यवस्थापनका लागि कानूनी र नीतिगत सुधारको दिशा निर्देश गर्दै, नेपालमा साइबर सुरक्षा सुदृढ गर्ने उपायहरूको चर्चा गरेको छ। लेखकले साइबर कसूर र सुरक्षा सम्बन्धी आवश्यक सुधारका लागि व्यावहारिक सुझावहरू प्रस्तुत गर्दै, कानूनी र नीतिगत सुधारका दिशा निर्देश गरेका छन्। समग्रमा, यो लेख नेपालमा साइबर सुरक्षा र कानूनी ढाँचामा सुधारका लागि महत्त्वपूर्ण सुझावहरू प्रदान गर्दछ, र साइबर कसूरका मुद्दामा सुधारको दिशा निर्देश गर्दछ।

६. A Study on Cyber Crime Cases in Nepal (Challenges and Recommendation २०२२) by National Judicial Academy

सैद्धान्तिक एवम् अनुसन्धानात्मक अध्ययन विधि प्रयोग गरिएको यस अध्ययनमा हाल लागू रहेको साईवर कानुनको प्रभावकारिता एवम् काठमाडौँ जिल्ला अदालतबाट मुद्दामा फैसला गर्दा सामना गर्नु परेका चुनौति पहिचान गरी आवश्यक सुधारको क्षत्र पहिल्याउने कार्य भएको छ। अध्ययनकर्ताले फैसला, जाहेरी, अभियोगपत्र समेतका आधारमा अध्ययन गरेको पाइयो। अध्ययन गर्दा वि.स. २०७८ साल सम्ममा काठमाडौँ जिल्ला अदालतमा चलेका मुद्दाहरुबाट तथ्याङ्क संकलन गरी साइवर क्राइम सम्बन्धि मुद्दाको न्याय निरुपणका क्रममा प्रहरी, वकिल र न्यायाशीशले सामना गर्नुपरेका समस्या र चुनौति पहिचान गरि आवश्यक सुझाव दिईएको छ।

प्रस्तुत लेखले काठमाडौँ जिल्ला अदालतमा साइबर कसूरका मुद्दाहरूको प्रभावकारिता र समस्याहरूको विश्लेषण गर्दछ । यस अध्ययनमा, लेखकले सैद्धान्तिक र अनुसन्धानात्मक विधिहरू प्रयोग गरेर, अदालतमा साइबर कसूरसम्बन्धी मुद्दा निपटाउने प्रक्रियामा देखिएका चुनौतीहरूको अध्ययन गरेका छन् । लेखमा, लेखकले काठमाडौँ जिल्ला अदालतमा साइबर कसूरका मुद्दा सुल्झाउँदा प्रहरी, वकिल र न्यायाधीशहरूले सामना गरेका समस्याहरूलाई पहिचान गर्दै, सुधारका लागि आवश्यक सुझावहरू प्रदान गरेका छन् । यस लेखले अदालतमा साइबर कसूरका मुद्दाहरूको न्यायिक व्यवस्थापनमा आएको समस्याहरू र चुनौतीहरूको विश्लेषण गर्दै, सुधारका लागि व्यावहारिक सुझावहरूको प्रस्तुति गरेको छ । लेखकले न्याय प्रक्रिया सुधारका लागि आवश्यक कदमहरूको चर्चा गर्दै, समग्र न्यायिक प्रणालीमा सुधार ल्याउने दिशामा मार्गदर्शन गरेको छ । यो अध्ययनले साइबर कसूरसम्बन्धी न्यायिक प्रक्रियामा सुधारका लागि आवश्यक सुझावहरू प्रदान गर्दै, न्यायिक व्यवस्थापनमा महत्वपूर्ण योगदान पुर्याउँछ । समग्रमा, यो लेख साइबर कसूरका मुद्दामा न्याय प्राप्तिमा सुधारका दिशामा महत्वपूर्ण मार्गदर्शन प्रदान गर्दछ ।

७. Cyber Crime and its Categories by Kejal Vadza (Article published in Indian Journal of Applied Research)

यस लेखमा विश्वव्यापी परिवेशमा घट्ने साईवर क्राइमको वर्गिकरण गरी उक्त कसूरहरु के कसरी गरिन्छन् भनि उल्लेख भएको छ । विशेषगरी साईवर कसूर दुई किसिमका हुन्छन्, कम्प्युटरलाई लक्षित गरी हुने गरेका कसूर र कम्प्युटरलाई प्रयोग गरी हुने गरेका कसूर भनि सामान्य वर्गिकरण गरिएको छ भने त्सयका अलावा अनअथोराईज्ड एक्सेस, ह्याकिङ र क्र्याकिङ, साईवर/अनलाईन ठगी, साईवर थेफ्ट, साईवर आतंकवाद, साईवर पोर्नोग्राफि, डिफेमेसन, साईवर स्टकिङ, ईमेल र आईआरसीसँग सम्बन्धि कसूर, आदी गरी २० वटा वर्गिकरण गरिएको छ ।

प्रस्तुत लेखले विश्वव्यापी साइबर कसूरको वर्गीकरण र तिनका विभिन्न प्रकारहरूको विस्तृत विश्लेषण प्रस्तुत गरेको छ । लेखकले यो लेखमा साइबर कसूरलाई दुई प्रमुख श्रेणीमा विभाजन गरेका छन्: कम्प्युटरलाई लक्षित गरिएका कसूर र कम्प्युटरलाई प्रयोग गरेर गरिने कसूरहरू । यस लेखले अनअथोराइज्ड एक्सेस, ह्याकिङ, क्र्याकिङ, साइबर ठगी, साइबर थेफ्ट, साइबर आतंकवाद, साइबर पोर्नोग्राफि, डिफेमेसन, साइबर स्टकिङ, र ईमेल तथा IRC सम्बन्धि कसूरहरूको विस्तृत वर्गीकरण प्रदान गरेको छ । लेखकले विभिन्न प्रकारका साइबर कसूरहरूको विश्लेषण गर्दै, तिनीहरूको प्रकृति र प्रभावहरूको चर्चा गरेका छन् । यस लेखले साइबर कसूरको वर्गीकरण र तिनका विशेषताहरूको अध्ययन गर्दै, कानूनी र सुरक्षात्मक उपायहरूको प्रस्तुति गरेको छ । समग्रमा, वड्जाको लेखले साइबर कसूरका विविध प्रकार र तिनका प्रभावहरूमा ध्यान दिन्छ, जसले कानूनी र सुरक्षात्मक उपायहरूको विकासमा मद्दत पुर्याउँछ ।

८. नेपालमा साइबर कसूर र यसको कानूनी चुनौतीहरू: बाबुराम अर्याल,गोरखापत्र,२०८०

यस लेखले नेपालमा साइबर कसूरको उदय र यससँग सम्बन्धित कानूनी चुनौतीहरूको समग्र विश्लेषण प्रस्तुत गरेको छ । लेखमा, लेखकले नेपालमा साइबर कसूरका घटनाहरूको वृद्धिको चर्चा गर्दै, यसले समाज र कानूनी प्रणालीमा उत्पन्न गरेका विविध समस्याहरूलाई उजागर गरेका छन् । यस अध्ययनमा, लेखकले साइबर कसूरका विभिन्न प्रकारहरू जस्तै फिसिंग, ह्याकिङ, र डेटा चोरीको विश्लेषण गर्दै, यी कसूरहरूको नियन्त्रण र रोकथाममा कानूनी ढाँचाको प्रभावकारिता मूल्याङ्कन गरेका छन् । लेखकले नेपालमा साइबर कसूर नियन्त्रणका लागि

लागू भएका कानूनी प्रावधानहरूको गहिरो अध्ययन गर्दै, तिनमा रहेका कमजोरी र समस्या क्षेत्रहरूको विश्लेषण गरेका छन्। नेपालमा साइबर कसूरका घटनामा वृद्धि हुँदै गएकाले, कानूनी प्रणाली र सुरक्षा संरचनामा सुधारको आवश्यकता रहेको निष्कर्षमा पुगेका छन्। लेखकले साइबर कसूरको बढ्दो चुनौतीसँग जुध्नका लागि आवश्यक कानूनी सुधार र नीतिगत उपायहरूको सुझाव दिएका छन्।

लेखमा, नेपालमा साइबर सुरक्षा प्रवर्द्धन गर्ने उद्देश्यले संस्थागत पहलहरू जस्तै साइबर ब्यूरो, सूचना सुरक्षा प्रतिक्रिया टोली, र अन्य सम्बन्धित संस्थाहरूको भूमिकाको पनि विश्लेषण गरिएको छ। लेखकले यी संस्थाहरूको कार्यक्षमता र उनीहरूले सामना गरेका चुनौतीहरूको मूल्याङ्कन गर्दै, सुधारका लागि आवश्यक सुझाव प्रस्तुत गरेका छन्। यस लेखले साइबर कसूर नियन्त्रण र कानूनी व्यवस्थापनमा देखिएका समस्याहरूको गहिरो विश्लेषण गर्दै, सुधारका लागि मार्गदर्शन गर्ने उद्देश्य राख्दछ। लेखकले कानूनी ढाँचामा देखिएका खामिहरूको विश्लेषण गर्दै, प्रभावकारी सुधारका सुझावहरू प्रदान गरेका छन्, जसले नेपालमा साइबर कसूरको व्यवस्थापनमा सुधार ल्याउने दिशामा महत्वपूर्ण योगदान पुर्याउँछ। यस अध्ययनले नेपालका कानूनी प्रावधानहरूको प्रभावकारिता र सुधारका आवश्यकताबारे स्पष्ट दृष्टिकोण प्रस्तुत गर्दै, साइबर कसूरको रोकथाम र व्यवस्थापनमा महत्वपूर्ण दिशानिर्देश प्रदान गर्दछ।

९. साइबर सुरक्षा कार्यान्वयन कार्य योजना, गृह मन्त्रालय

प्रस्तुत प्रतिवेदनले नेपालको साइबर सुरक्षा संरचनाको सुदृढीकरणका लागि आवश्यक रणनीतिहरू र कार्य योजना प्रस्तुत गर्दछ। यस रिपोर्टले साइबर सुरक्षा प्रणालीको स्थायित्व र प्रभावकारिता सुनिश्चित गर्नका लागि उठाइएका प्रमुख कदमहरू र सुझावहरूको समावेश गर्दछ। रिपोर्टमा, साइबर सुरक्षा रणनीतिका प्रमुख तत्वहरूको विश्लेषण गरिएको छ जसमा नेपालमा साइबर खतराहरूको विश्लेषण, प्रभावकारी सुरक्षा उपायहरूको विकास, र कानूनी ढाँचाको सुधार समावेश गरिएको छ। रिपोर्टले पहिलो चरणमा, नेपालको वर्तमान साइबर सुरक्षा परिदृश्यको मूल्याङ्कन गर्दै, प्रमुख सुरक्षा खतराहरू र चुनौतीहरूको विश्लेषण गरेको छ। यसमा, विभिन्न साइबर हमलाहरू, डेटा सुरक्षा उल्लंघन, र अन्य साइबर कसूरहरूको अध्ययन समावेश गरिएको छ। रिपोर्टले यी खतराहरूलाई व्यवस्थापन गर्नका लागि तत्काल कदमहरू चाल्नुपर्ने आवश्यकता औंल्याएको छ र यसका लागि आवश्यक संरचनात्मक सुधारहरूको चर्चा गरेको छ।

अर्को खण्डमा, रिपोर्टले साइबर सुरक्षा सुधारको लागि एक समन्वित रणनीतिक योजना प्रस्तुत गर्दछ। यस योजना अन्तर्गत, सूचना प्रविधिको सुरक्षित प्रयोग, जोखिम व्यवस्थापन, र घटना प्रतिक्रिया प्रक्रियाहरूको सुधार गर्नका लागि विभिन्न रणनीतिहरूको प्रस्ताव गरिएको छ। यसले साइबर सुरक्षा इन्फ्रास्ट्रक्चरको सुधार, राष्ट्रिय साइबर सुरक्षा नीति र कानूनी ढाँचामा आवश्यक सुधारका सुझावहरू प्रस्तुत गर्दछ। साथै, रिपोर्टले साइबर सुरक्षा कार्यान्वयनका लागि विभिन्न संस्थाहरूको भूमिकाको विश्लेषण पनि गरेको छ। यहाँ, राष्ट्रिय र स्थानीय स्तरमा साइबर सुरक्षा प्रवर्धन गर्ने उद्देश्यले बनाइएका संस्थागत संरचनाहरू, जस्तै साइबर ब्यूरो र सूचना सुरक्षा प्रतिक्रिया टोलीको विश्लेषण गरिएको छ। यी संस्थाहरूको कार्यक्षमता र सुधारको आवश्यकता बारेका सुझावहरू प्रस्तुत गरिएको छ। अन्तमा, रिपोर्टले कार्यान्वयन योजना र सुधारका उपायहरूको व्यावहारिकता मूल्याङ्कन गर्दै, सुदृढीकरणका लागि सुझावहरूको विस्तृत सूची प्रस्तुत गरेको छ। यसले साइबर सुरक्षा योजनाको प्रभावकारिता सुनिश्चित गर्न र सुरक्षित डिजिटल वातावरणको निर्माण गर्नका लागि मार्गदर्शन गर्दछ। समग्रमा, यो रिपोर्टले नेपालमा साइबर सुरक्षा सुधार र कार्यान्वयनका लागि एक समग्र दृष्टिकोण प्रस्तुत गर्दै, कानूनी, संरचनात्मक, र

रणनीतिक सुधारका लागि महत्वपूर्ण सुझावहरूको प्रस्तुति गरेको छ। यसले साइबर सुरक्षा कार्यान्वयनमा सुधार ल्याउने दिशामा महत्त्वपूर्ण दिशानिर्देशहरू प्रदान गर्दछ।

१०. नेपालमा साइबर सुरक्षा र यसको कानूनी चुनौतीहरू, प्रेमराज सिलवाल, नयाँपत्रिका

यस लेखले नेपालमा साइबर सुरक्षा र त्यससँग सम्बन्धित कानूनी चुनौतीहरूको समग्र विश्लेषण प्रस्तुत गरेको छ। लेखमा, लेखकले नेपालको वर्तमान साइबर सुरक्षा परिदृश्यमा रहेका प्रमुख समस्याहरू र चुनौतिहरूलाई उजागर गरेका छन्। लेखले प्रारम्भमा नेपालमा साइबर कसूरहरूको बढ्दो प्रवृत्ति र यसका कारणले उत्पन्न भएका समस्याहरूको विश्लेषण गरेको छ। यसमा, साइबर हमलाहरू जस्तै डेटा चोरी, फिसिंग, र ह्याकिङका घटनाहरूको वृद्धि र तिनका प्रभावहरूको चर्चा गरिएको छ। लेखकले यी समस्याहरूको समाधानका लागि कानूनी र नीतिगत सुधारको आवश्यकता औंल्याएका छन्।

रिपोर्टले साइबर सुरक्षा सुधारका लागि उठाइएका कदमहरूको पनि विश्लेषण गरेको छ। यसमा, सरकार र अन्य संलग्न संस्थाहरूले साइबर सुरक्षा संरचनाको सुदृढीकरणका लागि गरेका प्रयासहरूको अवलोकन गरिएको छ। लेखले साइबर सुरक्षा योजनाहरूको कार्यान्वयनमा भएका प्रगति र अवरोधहरूको चर्चा गर्दै, सुधारका लागि व्यावहारिक सुझावहरू प्रस्तुत गरेको छ। साथै, लेखमा, साइबर कसूर नियन्त्रणका लागि कानूनी प्रावधानहरूको मूल्याङ्कन गरिएको छ। यसले नेपालमा साइबर कसूरको कानूनी संरचनाको प्रभावकारिता र त्यसमा भएका समस्याहरूको विश्लेषण गर्दै, सुधारका लागि आवश्यक सुझावहरू प्रस्तुत गरेको छ। लेखकले कानूनी ढाँचामा देखिएका खामिहरू र तिनीहरूको सुधारका उपायहरूको विस्तृत विश्लेषण गरेका छन्।

लेखको अन्त्यमा, लेखकले साइबर सुरक्षा सुधारमा अगाडि बढ्नका लागि आवश्यक कदमहरूको एक समग्र सूची प्रस्तुत गरेका छन्। यसले नेपालमा साइबर सुरक्षा र कानूनी व्यवस्थापनका क्षेत्रमा सुधार ल्याउनका लागि मार्गदर्शन गर्ने उद्देश्य राख्दछ। यस लेखले नेपालमा साइबर सुरक्षा र कानूनी चुनौतीहरूको विस्तृत विश्लेषण प्रस्तुत गर्दै, सुधारका दिशानिर्देशहरू प्रदान गरेको छ। यसले साइबर सुरक्षा योजनाको प्रभावकारिता सुनिश्चित गर्न र सुरक्षित डिजिटल वातावरणको निर्माण गर्नका लागि महत्वपूर्ण सुझावहरूको प्रस्तुति गर्दछ।

११. Cybercrime and Cybercriminals: A Comprehensive Study, Regner Sabillon, Jeimy J. Cano M, Jordi Serra-Ruiz, Víctor Cavaller, ResearchGate,

यस अध्ययनले साइबर कसूर र साइबर अपराधीहरूको विस्तृत विश्लेषण प्रस्तुत गर्दछ। यो अध्ययनले साइबर कसूरका विभिन्न प्रकारहरू, अपराधीहरूको प्रवृत्ति, र यसलाई नियन्त्रण गर्ने उपायहरूको समग्र अध्ययन गर्दछ। अध्ययनले प्रारम्भमा साइबर कसूरको परिभाषा र यसको विकासक्रमलाई स्पष्ट पार्छ। यसमा, साइबर कसूरलाई दुई प्रमुख वर्गमा विभाजित गरिएको छ: एक त साइबर कसूर जुन कम्प्युटरलाई लक्ष्य बनाउँछ र अर्को, जसमा कम्प्युटरलाई कसूर गर्नको लागि प्रयोग गरिन्छ। लेखकले यी कसूरहरूको विश्लेषण गर्दै, ह्याकिङ, फिसिंग, मालवेयर आक्रमण, र डेटा चोरी जस्ता विशिष्ट प्रकारका साइबर कसूरहरूको चर्चा गरेका छन्।

अध्ययनले साइबर अपराधीहरूको विश्लेषण गर्दै, उनीहरूको मनोविज्ञान, प्रवृत्ति, र कार्यप्रणालीको गहिरो अध्ययन प्रस्तुत गरेको छ। यसले अपराधीहरूको सामाजिक र मनोवैज्ञानिक पृष्ठभूमिको मूल्याङ्कन गर्दै, उनीहरूले कसरी साइबर कसूरमा संलग्न हुने गर्छन् भन्ने कुरा स्पष्ट पार्दछ। लेखकले विभिन्न प्रकारका साइबर

अपराधीहरूको वर्गीकरण पनि गरेका छन्, जसमा अपराधिक समूहहरू, व्यक्तिगत अपराधीहरू, र राज्य प्रायोजित अपराधीहरू समावेश छन् ।

अध्ययनमा, साइबर कसूर नियन्त्रण र रोकथामका उपायहरूको विश्लेषण गर्दै, कानूनी र प्रविधि आधारित रणनीतिहरूको चर्चा गरिएको छ । यसमा, साइबर सुरक्षा उपायहरू, अनलाइन सुरक्षा शिक्षा, र कानूनी प्रावधानहरूको मूल्याङ्कन गरिएको छ । लेखकले प्रभावकारी नीतिहरू र कानूनी संरचनाहरूको विकासको आवश्यकता औंल्याएका छन् जसले साइबर कसूरको प्रभावकारी नियन्त्रण गर्न मद्दत पुर्याउन सक्छ । अन्तत, यो अध्ययनले साइबर कसूर र अपराधीहरूको गहिरो विश्लेषण गर्दै, सुधारका लागि विभिन्न सुझावहरू प्रदान गरेको छ । यसले कानूनी सुधार, प्रविधि उन्नति, र जनचेतना वृद्धि मार्फत साइबर कसूरको प्रभावकारी व्यवस्थापनमा महत्वपूर्ण योगदान पुर्याउँछ । सामान्य रूपमा, यो अध्ययनले साइबर कसूर र अपराधीहरूको विश्लेषणमा व्यापक दृष्टिकोण प्रस्तुत गर्दै, सुधार र नियन्त्रणका लागि रणनीतिक सुझावहरूको प्रस्तुति गरेको छ । यसले साइबर कसूर र सुरक्षा व्यवस्थापनमा एक समग्र दृष्टिकोण प्रस्तुत गर्दै, व्यावहारिक कदमहरूको दिशा निर्देश गर्दछ ।

१२. A Comprehensive Study on Cybersecurity and Cryptography, V Krishna Viraja and Pradnya Purandare, IOPscience

यस लेखले साइबर सुरक्षा र क्रिप्टोग्राफीका विविध पक्षहरूको विस्तृत विश्लेषण प्रस्तुत गर्दछ । लेखमा, साइबर सुरक्षा र क्रिप्टोग्राफीका सिद्धान्त र अभ्यासको गहिरो अध्ययन गरिएको छ, जसले आजको डिजिटल युगमा सुरक्षा र गोपनीयता सुनिश्चित गर्न महत्वपूर्ण भूमिका निभाउँछ । लेखले पहिलो खण्डमा साइबर सुरक्षा र यसको महत्वको विश्लेषण गर्दछ । यसमा, लेखकले विभिन्न साइबर खतराहरू र तीव्र रूपमा विकसित हुने साइबर कसूरहरूको चर्चा गर्दै, यो क्षेत्रको महत्व र चुनौतीहरूको विस्तृत वर्णन गरेका छन् । लेखकले साइबर सुरक्षा रणनीतिहरू, जोखिम मूल्याङ्कन विधिहरू, र सुरक्षा उपायहरूको व्याख्या गर्दै, सुरक्षित डिजिटल वातावरण निर्माणका लागि आवश्यक कदमहरूको सुझाव दिएका छन् । अर्को खण्डमा, क्रिप्टोग्राफीको भूमिकाको विश्लेषण गरिएको छ । यहाँ, लेखकले डेटा सुरक्षा र गोपनीयता सुनिश्चित गर्न प्रयोग गरिने विभिन्न क्रिप्टोग्राफी प्रविधिहरूको चर्चा गरेका छन् । यसमा, एन्क्रिप्शन र डिक्रिप्शन प्रक्रियाहरू, सार्वजनिक र निजी कुञ्जी क्रिप्टोग्राफी, र डिजिटल सिग्नेचरहरूको महत्त्व र प्रयोगहरूको विश्लेषण गरिएको छ । लेखकले क्रिप्टोग्राफीको विकास र यसको वर्तमान प्रवृत्तिहरूको पनि चर्चा गरेका छन्, जसले सूचना सुरक्षा र डेटा संरक्षित गर्न मद्दत गर्दछ ।

लेखको अन्तिम खण्डमा, लेखकले साइबर सुरक्षा र क्रिप्टोग्राफीका भविष्यका चुनौतीहरू र सम्भावनाहरूको विश्लेषण गरेका छन् । यसमा, नयाँ प्रौद्योगिकिहरू र प्रवृत्तिहरूको मूल्याङ्कन गर्दै, तिनीहरूले साइबर सुरक्षा र क्रिप्टोग्राफी क्षेत्रमा के प्रकारका सुधार र विकास ल्याउनेछन् भन्ने कुरामा ध्यान केन्द्रित गरिएको छ । लेखकले यी प्रवृत्तिहरूलाई ध्यानमा राख्दै, भविष्यमा साइबर सुरक्षा र क्रिप्टोग्राफीको दिशा निर्देश गर्ने सुझावहरू प्रस्तुत गरेका छन् ।

समग्रमा, यो लेखले साइबर सुरक्षा र क्रिप्टोग्राफीका सिद्धान्त र व्यवहारको समग्र विश्लेषण प्रस्तुत गर्दै, सुधार र विकासका लागि महत्वपूर्ण दिशानिर्देशहरू प्रदान गर्दछ । यसले डेटा सुरक्षा र गोपनीयता सुनिश्चित गर्नका लागि वर्तमान र भविष्यका चुनौतीहरूको व्यावहारिक समाधानहरू प्रस्तुत गर्दछ ।

परिच्छेद चार

साइवर कसूर सम्बन्धमा संवैधानिक, कानूनी, नीतिगत, संस्थागत, पद्धतिगत व्यवस्था तथा अनुसन्धान र अभियोजन

४.१. साइबर सुरक्षाका सम्बन्धमा नेपालमा भएका संवैधानिक, कानूनी, नीतिगत प्रयासहरू

नेपालमा सूचना प्रविधि तथा इन्टरनेटको बढ्दो प्रयोग सँग-सँगै सरकारी तवरबाट तथा निजीरूपमा पनि विभिन्न संघ संस्थाहरूबाट आ- आफ्नो तह र क्षमताबाट विभिन्न कार्यक्रमहरू ल्याई कार्यहरू हुँदै आएको पाइन्छ । सरकारी तहबाट साइबर सुरक्षालाई नियमन र नियन्त्रण गर्नका लागि नै भनेर कुनै कानून ल्याइएको अवस्था नभए तापनि विद्युतीय कारोबार ऐन, २०६३ मा यसको सुरुवात गर्न खोजिएको पाइन्छ भने मस्यौदाकै रूपमा भए तापनि सूचना प्रविधिसँग सम्बन्धित विधेयक र राष्ट्रिय साइबर सुरक्षा नीतिले यसका मुद्दाहरूलाई उठाएको पाइन्छ। निकट भविष्यमा यी मसौदाहरू कानूनका रूपमा परिणत हुने अपेक्षा राखिएको छ।

४.१.१. संवैधानिक व्यवस्था (Constitutional Provision)

नेपालको संविधानमा उल्लिखित मौलिक हकका केही व्यवस्थाहरू यस विषयसँग सम्बन्धित रहेको छ । जुन यस प्रकार छ।

१. सञ्चारको हक[१]

- विद्युतीय प्रकाशन, प्रसारण तथा छापा लगायतका जुनसुकै माध्यमबाट कुनै समाचार, सम्पादकीय, लेख, रचना वा अन्य कुनै पाठ्य, श्रव्य, श्रव्यदृश्य सामग्रीको प्रकाशन तथा प्रसारण गर्न वा सूचना प्रवाह गर्न वा छाप्न पूर्व प्रतिबन्ध लगाइने छैन । तर नेपालको सार्वभौमसत्ता, भौगोलिक अखण्डता, राष्ट्रियता वा संघीय इकाइबीचको सु–सम्बन्ध वा विभिन्न जात, जाति, धर्म वा सम्प्रदाय बीचको सु–सम्बन्धमा खलल पर्ने, राज्यद्रोह, गाली बेइज्जती वा अदालतको अवहेलना हुने वा कसूर गर्न दुरूत्साहन गर्ने वा सार्वजनिक शिष्टाचार, नैतिकताको प्रतिकूल कार्य गर्ने, श्रमप्रति अवहेलना गर्ने र जातीय छुवाछूत एवं लैंगिक भेदभावलाई दुरूत्साहन गर्ने कार्यमा मनासिब प्रतिबन्ध लगाउने गरी ऐन बनाउन रोक लगाएको मानिने छैन।

- कुनै श्रव्य, श्रव्यदृश्य वा विद्युतीय उपकरणको माध्यम वा छापाखानाबाट कुनै समाचार, लेख, सम्पादकीय, रचना, सूचना वा अन्य कुनै सामग्री मुद्रण वा प्रकाशन, प्रसारण गरे वा छापे बापत त्यस्तो सामग्री प्रकाशन, प्रसारण गर्ने वा छाप्ने रेडियो, टेलिभिजन, अनलाइन वा अन्य कुनै किसिमको डिजिटल वा विद्युतीय उपकरण, छापा वा अन्य सञ्चार माध्यमलाई बन्द, जफत वा दर्ता खारेज वा त्यस्तो सामग्री जफत गरिने छैन । तर यस उपधारामा लेखिएको कुनै कुराले रेडियो, टेलिभिजन, अनलाइन वा अन्य कुनै किसिमको

१ नेपालको संविधान, धारा १९

डिजिटल वा विद्युतीय उपकरण, छापाखाना वा अन्य सञ्चार माध्यमको नियमन गर्न ऐन बनाउन बन्देज लगाएको मानिने छैन।

- कानून बमोजिम बाहेक कुनै छापा, विद्युतीय प्रसारण तथा टेलिफोन लगायतका सञ्चार साधनलाई अवरूद्ध गरिने छैन।

२. छुवाछूत तथा भेदभाव विरूद्धको हक:[२]

- उत्पत्ति, जात, जाति वा शारीरिक अवस्थाको आधारमा कुनै व्यक्ति वा समुदायलाई उच्च वा नीच दर्शाउने, जात, जाति वा छुवाछूतको आधारमा सामाजिक भेदभावलाई न्यायोचित ठान्ने वा छुवाछूत तथा जातीय उच्चता वा घृणामा आधारित विचारको प्रचार प्रसार गर्न वा जातीय विभेदलाई कुनै पनि किसिमले प्रोत्साहन गर्न पाइने छैन।

३. गोपनीयताको हक:[३]

कुनै पनि व्यक्तिको जीउ, आवास, सम्पत्ति, लिखत, तथ्यांक, पत्राचार र चरित्र सम्बन्धी विषयको गोपनीयता कानून बमोजिम बाहेक अनतिक्रम्य हुनेछ।

४.१.२. कानूनी व्यवस्था (Legal Provision)

१. विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३

८० वटा दफा र १२ वटा परिच्छेद रहेको यस विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ नेपालमा विद्युतीय कारोबारलाई सम्वोधन गर्नको लागि जारी भएको विशेष ऐन हो। यस ऐनको प्रस्तावनामा विद्युतीय तथ्याङ्क आदान–प्रदानको माध्यमबाट वा अन्य कुनै विद्युतीय सञ्चार माध्यमबाट हुने कारोबारलाई भरपर्दो र सुरक्षित बनाई विद्युतीय अभिलेखको सृजना, उत्पादन, प्रशोधन, सञ्चय, प्रवाह तथा सम्प्रेषण प्रणालीको मान्यता, सत्यता, अखण्डता र विश्वसनीयतालाई प्रमाणीकरण तथा नियमित गर्ने व्यवस्था गर्न र विद्युतीय अभिलेखलाई अनधिकृत तवरबाट प्रयोग गर्न वा त्यस्तो अभिलेखमा गैरकानूनी तवरबाट परिवर्तन गर्ने कार्यलाई नियन्त्रण गर्नका लागि कानूनी व्यवस्था गर्न जारी भएको भन्ने उल्लेख गरिएबाट मूलतः यो ऐन विद्युतीय दस्तखत (Digital Signature) को प्रचलन र विश्वसनीयताको लागि कार्यान्वयनमा ल्याइएको देखिन्छ। तथापी हालको अवस्थामा नेपालमा साइवर कसूरलाई नियन्त्रण गर्नको लागि समेत विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ नै कार्यान्वयनमा रहेको अवस्था छ। यस ऐनको परिच्छेद ९ मा रहेको कम्प्युटर सम्बन्धी कसूर अन्तर्गत दफा ४४ देखि ५९ सम्म उल्लिखित प्रावधानहरू साइवर कसूरको विषयसँग सम्बन्धित रहेको देखिन्छ।

नेपालको वर्तमान परिप्रेक्ष्यमा यो ऐन नेपालको सूचना प्रविधिको क्षेत्रमा तथा यससँग सम्बन्धित कसूरहरूको नियमन र नियन्त्रण गर्नका लागि आवश्यक प्रमुख कानूनको रूपमा रहेका छ। यस ऐनमा साइबर सुरक्षाको सम्बन्धमा व्यवस्था गर्नका लागि कुनै पनि छुट्टै दफामा व्यवस्था नगरिएको भए तापनि साइबर स्पेस (Cyber

२ नेपालको संविधान, धारा २४(३)

३ नेपालको संविधान, धारा २८

Space) वा हुने गरेका कसूरहरू नियन्त्रण त्यस्ता अपराधीहरूलाई सजाय गर्नका लागि परिच्छेद ९ मा कम्प्युटरसम्बन्धी कसुरअन्तर्गत दफा ४४ देखि दफा ५९ सम्म विभिन्न व्यवस्थाहरू गरेको पाइन्छ।

- दफा ४४. कम्प्युटर स्रोत सङ्केतको चोरी, नष्ट वा परिवर्तन गर्ने
- दफा ४५. कम्प्युटर सामग्रीमा अनधिकृत पहुँच
- दफा ४६. कम्प्युटर र सूचना प्रणालीमा क्षति पु¥याउने
- दफा ४७. विद्युतीय स्वरुपमा गैरकानूनी कुरा प्रकाशन गर्ने
- दफा ४८. गोपनीयता भङ्ग गर्ने
- दफा ४९. झुट्ठा व्यहोराको सूचना दिने
- दफा ५०. झुट्ठा इजाजतपत्र वा प्रमाणपत्र पेश गर्ने वा देखाउने
- दफा ५१. तोकिएको विवरण वा कागजात दाखिला नगर्ने
- दफा ५२. कम्प्युटर जालसाजी गर्ने
- दफा ५३. कम्प्युटर सम्बन्धी कसूर गर्न दुरुत्साहन
- दफा ५४. मतियारलाई सजाय
- दफा ५५. नेपाल राज्यबाहिर गरेको कसूरमा हुने सजाय
- दफा ५६. जफत गर्ने
- दफा ५७. सङ्गठित संस्थाले गरेको कसूर
- दफा ५८. अन्य सजाय
- दफा ५९. प्रचलित कानून बमोजिम सजाय गर्न बाधा नपुग्ने

यसरी साइबर कसूरको नियमन र नियन्त्रण साइबर सुरक्षाका लागि प्रारम्भिक कदम भएको हुनाले यसलाई साइबर सुरक्षाको आधारविन्दु मान्न सकिन्छ। यति कुरा गर्दा गर्दै पनि ऐनको दफाहरूमा साइबर सुरक्षालाई परिभाषित नगरिएको र सोसँग सम्बन्धित व्यवस्थाहरूलाई नसमेटिएको भए तापनि सो ऐनको प्रस्तावनामा गरिएको व्यवस्थाबाट यो ऐन आउनुको एउटा उद्देश्य साइबर सुरक्षा पनि हो भन्ने कुरा प्रस्ट हुन्छ। ऐनको परिच्छेद ५ को दफा ३० देखि ३४ सम्म गरिएको डिजिटल हस्ताक्षर तथा प्रमाणपत्रसम्बन्धी व्यवस्थालाई र परिच्छेद ७ को विद्युतीय अभिलेख र डिजिटल हस्ताक्षरको सरकारी प्रयोग ६ शीर्षक अन्तर्गत दफा ४१ मा गरिएको व्यवस्थाबाट सरकारी निकाय वा सार्वजनिक संस्था वा नेपाल राज्यभित्र कारोबार गर्ने बैङ्क वा वित्तीय संस्थामा विद्युतीय रूपमा कारोबार हुँदा डिजिटल हस्ताक्षरको प्रयोग गरी त्यस्ता कारोबारहरूलाई साइबर खतराको दृष्टिकोणबाट सुरक्षित बनाउन सकिने भन्ने कुरा पुष्टि हुन्छ भने यसले कम्तीमा नेपालको सरकारी तथा अन्य निजी बैङ्क र वित्तीय संस्थाहरूबाट आर्थिक कारोबार गर्दा जोखिम र त्यसको साइबर सुरक्षालाई समेटेको पाइन्छ।

यस विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ ले अपराधीकरण गरेका कसूरहरूलाइ यस प्रकार उल्लेख गर्न सकिन्छ।

- **कम्प्युटर स्रोत सङ्केतको चोरी, नष्ट वा परिवर्तन गर्ने**: प्रचलित कानूनले कम्प्युटर स्रोतको सङ्केत (सोर्स

कोड) लाई यथावत् राख्ने गरी तत्काल व्यवस्था गरेको अवस्थामा कुनै व्यक्तिले कुनै कम्प्युटर, कम्प्युटर कार्यक्रम, कम्प्युटर प्रणाली वा कम्प्युटर नेटवर्कका लागि प्रयोग हुने कम्प्युटर स्रोतको सङ्केत (सोर्स कोड) लाई जानी–जानी वा बदनियत राखी चोरी गरेमा, नष्ट गरेमा, परिवर्तन गर्ने कार्य[४]

- **कम्प्युटर सामग्रीमा अनधिकृत पहुँच: कुनै** व्यक्तिले कुनै कम्प्युटरमा रहेको कुनै कार्यक्रम, सूचना वा तथ्याङ्कमा पहुँच प्राप्त गर्ने मनसायबाट सो कम्प्युटरको धनी वा जिम्मेवार व्यक्तिबाट कुनै अख्तियारी नलिई सो कम्प्युटरको प्रयोग गरेमा वा अख्तियारी लिएको अवस्थामा पनि अख्तियारी दिइएको भन्दा भिन्न कुनै कार्यक्रम, सूचना वा तथ्याङ्कमा पहुँच प्राप्त गर्ने उद्देश्यले गरेको कुनै कार्य[५]

- **कम्प्युटर र सूचना प्रणालीमा क्षति पुर्‍याउने:** कुनै व्यक्तिले कुनै संस्थालाई गलत तरिकाले हानि नोक्सानी पुर्‍याउने मनसाय राखी जानी–जानी कम्प्युटर सम्पदामा रहेको कुनै सूचनालाई कुनै पनि व्यहोराबाट नष्ट गरेमा, क्षति पुर्‍याएमा, मेटाएमा, हेरफेर गरेमा, काम नलाग्ने बनाएमा वा त्यस्तो सूचनाको मूल्य र प्रयोगको महत्वलाई ह्रास गराएमा वा हानिकारक प्रभाव पारेमा वा कसैलाई त्यस्तो काम गर्न लगाएमा[६]

- **विद्युतीय स्वरूपमा गैरकानूनी कुरा प्रकाशन गर्ने:**[७] कम्प्युटर, इन्टरनेट लगायतका विद्युतीय सञ्चार माध्यमहरूमा प्रचलित कानूनले प्रकाशन तथा प्रर्दशन गर्न नहुने भनी रोक लगाएका सामग्रीहरू वा सार्वजनिक नैतिकता, शिष्टाचार विरूद्धका सामग्री वा कसैप्रति घृणा वा द्वेष फैलाउने वा विभिन्न जात जाति र सम्प्रदायबीचको सुमधुर सम्बन्धलाई खलल पार्ने किसिमका सामग्रीहरू प्रकाशन वा प्रदर्शन गर्ने, महिलालाई जिस्क्याउने, हैरानी गर्ने, अपमान गर्ने वा यस्तै अन्य कुनै किसिमको अमर्यादित कार्य गर्ने वा गर्न लगाएमा

- **गोपनीयता भङ्ग गर्ने:**[८] यो ऐन वा यस ऐन अन्तर्गत बनेका नियमहरू वा प्रचलित कानूनमा अन्यथा व्यवस्था भएकोमा बाहेक यो ऐन वा यस ऐन अन्तर्गत बनेका नियमहरू अन्तर्गत प्रदान गरिएको कुनै अधिकार बमोजिम कुनै विद्युतीय अभिलेख, किताब, रजिष्टर, पत्रव्यवहार, सूचना, कागजात वा अन्य सामग्रीहरूमा पहुँच प्राप्त गरेको कुनै व्यक्तिले कुनै अनधिकृत व्यक्तिलाई त्यस्तो अभिलेख, किताब, रजिष्टर, पत्र व्यवहार, सूचना, कागजात वा सामग्रीको गोपनीयता भङ्ग गरेमा वा भङ्ग गर्न लगाएमा

- **झुट्टा व्यहोराको सूचना दिने:**[९] कुनै व्यक्तिले प्रमाणीकरण गर्ने निकायको इजाजतपत्र प्राप्त गर्ने वा अन्य कुनै मनसायले नियन्त्रक समक्ष वा डिजिटल हस्ताक्षर प्रमाणपत्र प्राप्त गर्ने वा अन्य कुनै मनसायले प्रमाणीकरण गर्ने निकाय समक्ष पेश गर्ने कुनै व्यहोरा जानी-जानी लुकाएमा वा ढाँटेमा वा जानाजानी झुट्टा व्यहोरा पेश वा दाखिला गरेमा

- **कम्प्युटर जालसाजी गर्ने:**[१०] कुनै व्यक्तिले कुनै जालसाजी गर्ने वा अन्य कुनै गैरकानूनी कार्य गर्ने उद्देश्यले

---

४ विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ४४
५ विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ४५
६ विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ४६
७ विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ४७(१)
८ विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ४८
९ विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ४९
१० विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ५२

डिजिटल हस्ताक्षर प्रमाणपत्र सृजना गरेमा, प्रकाशन गरेमा वा अन्य व्यहोराले उपलब्ध गराएमा वा कुनै बिलको भुक्तानी रकम, कसैको खाताको बाँकी मौज्दात (ब्यालेन्स), कुनै आपूर्ति र भण्डार (इन्भेण्टरी) वा जुनसुकै बखत भुक्तानी दिने कार्ड (ए.टी.एम.कार्ड) मा मिलोमतो गरी वा अन्य कुनै तरिकाले जालसाजी गरी लाभ उठाएमा

- **नेपाल राज्यबाहिर गरेको कसूरमा हुने सजाय**:[११] प्रचलित कानूनमा जुनसुकै कुरा लेखिएको भए तापनि कुनै व्यक्तिले यस ऐन बमोजिम कसूर हुने कुनै काम नेपाल राज्यबाहिर रहेर गरेको भए तापनि त्यस्तो कसूर गरिएको कम्प्युटर, कम्प्युटर प्रणाली वा कम्प्युटर नेटवर्क प्रणाली नेपालमा अवस्थित भएमा त्यस्तो कसूर गर्ने व्यक्तिलाई यस ऐन बमोजिम मुद्दा चलाई सजाय गर्न सकिने।

- **सङ्गठित संस्थाले गरेको कसूर**:[१२] यस ऐन बमोजिम कसूर ठहर्ने कुनै कुरा सङ्गठित संस्थाले गरेमा सो कसूर गर्दाका बखत सो सङ्गठित संस्थाको सञ्चालनको लागि प्रमुख रूपमा जिम्मेवार व्यक्तिले सो कसूर गरेको मानिने।

- यस कसूरको दुरूत्साहन र मतियार कार्य लाई पनि अपराधीकरण गरेको छ।

- **न्यायाधिकरणको गठन**:[१३] नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी परिच्छेद–९ मा उल्लेख भए बमोजिमका कसूरहरूको शुरू कारबाही र किनारा गर्न कानून सदस्य, सूचना प्रविधि सदस्य र वाणिज्य सदस्य भएको तीन सदस्यीय सूचना प्रविधि न्यायाधिकरणको गठन गर्नेछ। यस दफामा अन्यत्र जुनसुकै कुरा लेखिएको भए तापनि उपदफा (१) बमोजिम न्यायाधिकरण गठन नभएसम्मकालागि परिच्छेद–९ मा उल्लेख भए बमोजिमका कसूरहरूको शुरू कारबाही र किनारा गर्ने क्षेत्राधिकार नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी तोकिदिएको जिल्ला अदालतलाई हुनेछ। उपरोक्त कानूनी व्यवस्था अनुरूप नेपाल सरकारले मिति २०६४।१२।२५ मा निर्णय गरी विद्युतीय कसूर सम्बन्धी मुद्दा हेर्ने गरी काठमाडौं जिल्ला अदालतलाई क्षेत्राधिकार तोकिएको छ। हाल सम्म पनि विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ६० मा उल्लिखित प्रावधान अनुरूप न्यायाधीकरणको गठन भइ नसकेको हुँदा काठमाडौं जिल्ला अदालतबाट नै साइवर कसूर सम्बन्धी मुद्दाको सुनुवाई र किनारा भइरहेको छ।

- **पुनरावेदन न्यायाधिकरणको स्थापना र गठन**:[१४] नेपाल सरकारले नेपाल राजपत्रमा सूचना प्रकाशन गरी न्यायाधिकरणले गरेको निर्णय वा आदेश उपर पुनरावेदन सुन्न र यस ऐन बमोजिम नियन्त्रक वा प्रमाणीकरण गर्ने निकायले गरेको निर्णय वा आदेश उपर पुनरावेदन सुन्न दफा ६७ बमोजिमको योग्यता पुगेका व्यक्तिहरू मध्ये बाट कानून सदस्य, सूचना प्रविधि सदस्य र वाणिज्य सदस्य भएको तीन सदस्यीय सूचना प्रविधि पुनरावेदन न्यायाधिकरणको गठन गर्नेछ।

२. मुलुकी अपराध संहिता, २०७४

मुलुकी अपराध संहिता, २०७४ को भाग ३ को गोपनीयता विरूद्धको कसुरहरू अन्तर्गत उल्लेख गरिएका

११ विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ५५
१२ विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ५७
१३ विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ६०
१४ विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ६६

प्रावधानहरू पनि साइवर कसूरसँग सम्बन्धित रहेको छ । यस ऐनले अपराधीकरण गरेका साइवर कसूरसँग सम्बन्धीत कसूरहरू यस प्रकार रहेका छन् ।

- अर्काको कुरा सुन्न वा ध्वनी अङ्कन गर्न नहुने:[१५] कसैले दुई वा दुईभन्दा बढी व्यक्तिहरूका बीचमा भएका कुनै कुरा अधिकार प्राप्त अधिकारीको अनुमतिले वा त्यसरी कुरा गर्ने व्यक्तिहरूको मञ्जुरी विना कुनै यान्त्रिक उपकरणको प्रयोग गरेर सुन्न वा त्यस्तो कुराको ध्वनी अङ्कन गर्न नहुने ।
- गोप्य कुरा प्रकट गर्न नहुने:[१६] कसैले आफ्नो व्यावसायिक कामको सिलसिलामा कुनै व्यक्तिबाट थाहा पाएको निजको कुनै गोप्य कुरा कानूनले वाध्य गराएको वा त्यस्तो व्यक्तिले अनुमति दिएको अवस्थामा बाहेक कसैलाई पनि प्रकट गर्न नहुने ।
- अनुमति विना कुनै व्यक्तिको तस्विर खिच्न वा तस्वीरको स्वरूप बिगार्न नहुने:[१७]
- कसैले कुनै व्यक्तिको अनुमति विना निजको तस्विर खिच्न वा निजको तस्विरसँग अरू कसैको तस्विर राखी अर्को तस्विर बनाउन नहुने ।
- कसैले एकको तस्विरको केही भाग अर्को व्यक्तिको अर्को भागसँग राखी वा अन्य कुनै किसिमले विकृत रूपको तस्विर बनाउन वा प्रकाशन गर्न नहुने ।
- चिठ्ठी खोल्न वा टेलिफोनमा गरेको कुरा सुन्न नहुने:[१८] अधिकार प्राप्त अधिकारी वा सम्बन्धित व्यक्तिको अनुमति विना कसैको चिठ्ठी खोल्न वा अरूले टेलिफोनमा गरेको कुरा कुनै यान्त्रिक उपकरणको प्रयोग गरेर बीचमा सुन्न वा ध्वनी अङ्कन गर्न नहुने ।
- विद्युतीय माध्यमद्वारा गोपनीयता भङ्ग गर्न नहुने:[१९] कसैले विद्युतीय माध्यममा रहेको वा प्रवाह हुने सूचना, जानकारी, पत्राचार अनधिकृत रूपमा प्राप्त गर्न त्यसको गोपनीयता भङ्ग गर्न वा अनधिकृत रूपमा कसैलाई हस्तान्तरण गर्न वा गराउन नहुने ।
- छलकपटपूर्ण टेलिफोन वा सन्देश प्रवाह गर्न नहुने:[२०] कसैले आफ्नो परिचय दिई वा नदिई कसैलाई छल्ने, धोका दिने, हैरानी पार्ने वा सताउने उद्देश्यले छलकपट पूर्ण टेलिफोन वा सन्देश प्रवाह गर्न गराउन नहुने ।

३. प्रस्तावित सूचना प्रविधि विधेयक, २०७५ :

साइबर जगतको नियन्त्रण, सञ्चालन र अनुगमनको लागि विस्तृत कानून तयार पारी जारी गर्ने उद्देश्य सहित सूचना प्रविधि विधेयक, २०७५ तयार भएको थियो । सरोकारवाल निकायहरू, प्रतिपक्ष दलहरूबाट समेत व्यापक विरोधका कारण उक्त विधेयक पास हुन सकेन । यस विधेयकमा भएका विधिशास्त्रीय विरोधाभास, द्विविधात्मक

१५ मुलुकी अपराध संहिता, २०७४, दफा २९३
१६ मुलुकी अपराध संहिता, २०७४, दफा २९४
१७ मुलुकी अपराध संहिता, २०७४, दफा २९५
१८ मुलुकी अपराध संहिता, २०७४, दफा २९७
१९ मुलुकी अपराध संहिता, २०७४, दफा २९८
२० मुलुकी अपराध संहिता, २०७४, दफा २९९

वाक्यांशका कारण सरोकारवालाहरूबाट विरोध भएको हुँदा पारित हुन सकेन । यस विधेयकको प्रस्तावनामा सूचना प्रविधिको विकास, प्रर्बद्धन र नियमन गर्न, विद्युत्तीय अभिलेख तथा हस्ताक्षरको मान्यता, सत्यता र विश्वासनीयतालाई नियमन गर्न, विद्युतीय माध्यमबाट सार्जजनिक सेवा प्रवाह गर्न, साइबर सुरक्षाको समुचित व्यवस्था गरी साइबर कसूरलाई नियन्त्रण गरी सर्वसाधारणको हित कायम गर्न तथा सामाजिक सञ्जालको प्रयोगलाई व्यवस्थित र मर्यादित बनाउने सम्बन्धमा आवश्यक कानूनी व्यवस्था गर्न प्रचलित कानूनलाई संशोधित र एकीकरण गर्न प्रस्तुत विधेयकको निर्माण गरिएको भन्ने उल्लेख छ । प्रत्येक प्रदेशमा सूचना प्रविधि सम्बन्धी अदालत स्थापना गर्ने, सामाजिक सञ्जाल दर्ता र नियमन, चरित्र हत्या गने उर्देश्यले वा प्रचलित कानून बमोजिम गाली बेइज्जति मानिने कुनै कार्य गर्न नहुने, विद्युतीय अभिलेख सम्बन्धी व्यवस्था, विद्युतीय माध्यमबाट सेवा प्रवाह गर्ने लगायतका विभिन्न प्रावधानहरू समावेश गरी सूचना प्रविधी सम्बन्धी विधेयक. २०७५ तयार गरिएको थियो ।

यो विधेयक विधायिकामा विचारधीन र छलफलकै क्रममा रहेको भए तापनि यसको प्रस्तावना, यसमा गरिएको साइबर सुरक्षाको परिभाषा र यसमा भएका साइबर सुरक्षासम्बन्धी केही व्यवस्थाहरूले नेपालले छिट्टै नै साइबर सुरक्षा र यसको आवश्यकतालाई आत्मसात गरी यस क्षेत्रमा एक कदम अगाडि बढ्न प्रयास गर्न खोजेको आभाष हुन्छ । यस विधेयकको प्रस्तावनामा सूचना प्रविधिको विकास, प्रवर्द्धन र नियमन गर्न, विद्युतीय अभिलेख तथा हस्ताक्षरको मान्यता, सत्यता र विश्वसनीयतालाई नियमन गर्न, विद्युतीय माध्यमबाट सार्वजनिक सेवा प्रवाह गर्न, साइबरसुरक्षाको समुचित व्यवस्था गरी साइबर कसूरलाई नियन्त्रण गरी सर्वसाधारणको कायम गर्न तथा सामाजिक सञ्जालको प्रयोगलाई व्यवस्थित र मर्यादित बनाउने सम्बन्धमा आवश्यक कानूनी व्यवस्था गर्न भनी उल्लेख गरेको छ । ५७ यस व्यवस्थाबाट यस विधेकले साइबर सुरक्षा पनि यसको उद्देश्यहरूमध्ये एक रहेको भन्ने कुरालाई पुष्टि गर्दछ । विधेयकको दफा १(भ) मा साइबर सुरक्षा भन्नाले कुनै पनि सूचना प्रविधिमा आधारित प्रणाली, नेटवर्क र प्रोगामलाई डिजिटल आक्रमणबाट सुरक्षा गर्ने अभ्यास सम्झिनुपर्दछ भनी साइबर सुरक्षाको फराकिलो परिभाषा गरेको पाइन्छ । त्यसै गरी परिच्छेद १२ लाई साइबर सुरक्षासम्बन्धी व्यवस्था भनी छुट्टै नामकरण र व्यवस्था गर्दै प्रस्तावनाको उद्देश्यलाई यसमार्फत पूरा गरेको पाइन्छ । यस परिच्छेदअन्तर्गत गरिएका साइबर सुरक्षासम्बन्धी व्यवस्थाहरूमा दफा ७९ मा नेपाल सरकारले कुनै पनि राष्ट्रिय सुरक्षा, अर्थव्यवस्था, अत्यावश्यक सेवा, आकस्मिक सेवा, स्वास्थ्य वा सार्वजनिक सुरक्षासमेतमा गम्भीर असर पुऱ्याउन सक्ने सूचना तथा सञ्चार पूर्वाधारहरूलाई नेपाल राजपत्रमा सूचना प्रकाशन गरी संवेदनशील पूर्वाधार तोक्न सक्ने ९ भन्ने व्यवस्था र दफा ८० साइबर सुरक्षासम्बन्धी घटनामा तत्काल सहायताका लागि मन्त्रालयमा तोकिएबमोजिमको एक नेपाल सूचना प्रविधि आकस्मिक सहायता समूहको व्यवस्था रहनेछ भनी व्यवस्था गरेको पाइन्छ यस व्यवस्थालाई अन्तर्राष्ट्रिय रूपमा समेत अवलम्बन गरिएका महत्त्वपूर्ण व्यवस्थाको रूपमा लिन सकिन्छ ।

त्यस्तै विधेयकको परिच्छेद ११ मा सूचना सुरक्षाको समेत व्यवस्था गरिइएको छ । विद्युतीय स्वरूपमा रहेका सूचनाको आदान प्रदान, प्रशोधन तथ संचय गर्दा प्रशोधनकर्ता, सञ्चयकर्ता तथा सेवा प्रदायकले गोपनीयता र अक्षुण्णता कायम गरी गर्नु पर्ने;१ सरकारी, सार्वजनिक, वित्तीय तथा स्वास्थ्य सम्बन्धी निकायले तोकिएको विवरण अनिवार्य रूपमा तोकेअनुसार इन्क्रिप्सन गरी राख्नु पर्ने;६२ सरकारी, सार्वजनिक, वित्तीय तथा स्वास्थ्यसम्बन्धी निकायले तोकिएको विवरण प्रशोधन, सम्प्रेशण र भण्डारण गर्दा सूचना नेपालबाहिर नजाने गरी सुरक्षित राख्नु पर्ने र सूचना सुरक्षासम्बन्धी अन्य व्यवस्था तोकिए गर्नु पर्ने ४ भनी सूचना सुरक्षासम्बन्धी प्रत्यभूति गर्नुपर्ने व्यवस्था

गरेको पाइन्छ। त्यस्तै सरकारी निकायले कम्प्युटर तथा सूचना प्रणाली प्रयोग गर्दा मन्त्रालयले तोकेको मापदण्ड अवलम्बन गर्नुपर्ने ५ भनिसमेत व्यवस्था गरेको छ। यसैगरी सरकारी, सार्वजनिक, वित्तीय तथा स्वास्थ्यसम्बन्धी सूचना प्रयोग गर्ने संस्थाहरूले अनिवार्य रूपमा आफूले प्रयोग गर्ने सूचना प्रविधि प्रणालीको तोकिएबमोजीमको अवधिमा सुरक्षा परीक्षण गराउनुपर्ने भनी सुरक्षा परीक्षण सम्बन्धीसमेत व्यवस्था गरेको पाइन्छ।

४. वैयक्तिक गोपनीयतासम्बन्धी ऐन, २०७५

वैयक्तिक गापनीयतासम्बन्धी ऐन, २०७५ को परिच्छेद - १० मा वैयक्तिक सूचना सङ्कलन तथा संरक्षणसम्बन्धी व्यवस्था गरिएको छ। ऐनको दफा २५ मा सङ्कलित सूचनाको संरक्षणसम्बन्धी व्यस्था गरिएको छ जसअनुसार कुनै सार्वजनिक निकायले सङ्कलन गरेको वा त्यस्तो निकायको जिम्मा वा नियन्त्रणमा रहेको वैयक्तिक सूचना त्यस्तो निकायले संरक्षण गर्नु पर्नेछ" भन्ने व्यवस्थाबाट विद्युतीय सूचनाहरूको साइबर सुरक्षामा ध्यान केन्द्रित गरेको भए तापनि किसिमको कानूनी व्यवस्थाले प्रइभेट कम्पनीहरूले सुरक्षामा केन्द्रित नरहेपनि हुने छुट दिएको बुझिन्छ।

५. विद्युतीय कारोबार नियमावली, २०६४

विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ को दफा ७८ मा उल्लिखित प्रावधान अनुरूप विद्युतीय कारोबार नियमावली, २०६४ जारी गरि कार्यान्वयनमा आएको छ। २०६४। ४। २१ देखि लागू यस नियमावलीमा ६ परिच्छेद, ४२ नियम, ६ वटा अनुसूचीहरू समावेश छन्। यसै नियमावलीको आधारमा नेपालमा विद्युतीय हस्ताक्षर (डिजीटल सिग्नेचर) को शुभारम्भ भएको छ।

६. साइबर सुरक्षा विनियमावली, २०७७

नेपाल दुरसञ्चार प्राधिकरणले लागू गरेको 'साइबर सुरक्षा विनियमावली, २०७७' मा सञ्चार प्रविधिका पूर्वाधार लगायत सूचना प्रणालीलाई विभिन्न प्रकारका साइबर आक्रमणबाट जोगाउन प्राधिकरणबाट अनुमतिपत्र प्राप्त सबै दूरसञ्चार सेवा प्रदायकहरू (आधारभूत दूरसञ्चार, टेलिफोन, मोबाइल नेटवर्क, इन्टरनेट लगायत) ले अन्तर्राष्ट्रिय रूपमा प्रचलित मापदण्ड तथा अभ्यास अनुसार सुरक्षाका विषयमा गर्नुपर्ने कार्यहरू, सेवाप्रदायकले गोप्य राख्नुपर्ने ग्राहकका सूचना, प्रयोग गर्नुपर्ने सफ्टवेयर तथा सबै सिष्टमहरू लगायत सेवाप्रदायकले आइपि अडिट गरी तीन देखि ६ महिनामा प्राधिकरणमा बुझाउनुपर्ने, बुझाइएको लेखापरीक्षण प्रतिवेदनमा प्राधिकरणले क्रस चेक समेत गर्न सक्ने व्यवस्था सम्बन्धमा उल्लेख गरिएको छ।

७. सूचना प्रविधि आकस्मिक सहायता समूह (सञ्चालन तथा व्यवस्थापन) निर्देशिका, २०७५

सूचना प्रविधिको विकास तथा बढ्दो प्रयोग सँगै देखिएको साइबर सुरक्षा जोखिमको पहिचान, त्यसबाट हुने असरको न्यूनीकरण र आकस्मिक साइबर सुरक्षाको व्यवस्था गर्न उपयुक्त संयन्त्र गठन, सञ्चालन तथा व्यस्थापन सम्बन्धमा व्यवस्था गरिएको।

८. अनलाइन बालसुरक्षा निर्देशिका, २०७६

सूचना तथा सञ्चार प्रविधिको विकाससँगै अनलाइन माध्यममा बालबालिकामाथि बढ्दो दुर्व्यवहारका घटनालाई सरोकारवालाहरूको संयुक्त पहलबाट न्यूनीकरण गर्न तथा बालबालिकाको लागि इन्टरनेटको सुरक्षित प्रयोगको

लागि दूरसञ्चार ऐन, २०५३ को दफा १३ बमोजिम यो निर्देशिका बनाइएको हो। सेवा प्रदायकले गर्नुपर्ने कार्य (गैरकानुनी तथा हानिकारक सामग्रीको उपलब्धता न्यूनीकरण, बाल दुर्व्यवहारजन्य सामग्री तुरुन्त हटाउने, त्यस्ता सामग्री वा लिङ्क उजुरी गर्ने संरचना विकास, सेवा प्रदायकले उपलब्ध गराएको सेवा तथा सामग्रीमा उमेर समूह स्पष्ट अवगत हुने व्यवस्था सम्बन्धी), घरपरिवार तथा समाजले गर्नुपर्ने कार्य (कम्प्युटरको सुरक्षित प्रयोग, कम्प्युटरको सुरक्षित प्रयोग सम्बन्धमा अभिमुखीकरण गर्ने, बालबालिकाले प्रयोग गर्ने वेबसाइट तथा एप्सको जानकारी राख्ने, विद्यालयको कम्प्युटरमा इन्टरनेटको सुरक्षित प्रयोग गर्नुपर्ने, सरोकारवाला संस्थाहरूको दायित्व सम्बन्धी), तथा नेपाल दूरसञ्चार प्राधिकरणले गर्ने कार्य सम्बन्धमा उल्लेख गरिएको छ।

९. यस बाहेक कम्पनी ऐन, २०६३, प्रतिलीपी अधिकार ऐन, २०५९, पेटेण्ट डिजाइन र ट्रेडमार्क ऐन, २०२२, आवश्यक सेवा सञ्चालन ऐन, २०१४, आवश्यक वस्तु संरक्षण ऐन, २०१२, छापाखाना र प्रकाशन सम्बन्धी ऐन, २०४८, प्रेस काउन्सिल ऐन, २०४८, राष्ट्रिय प्रसारण ऐन, २०४९, दुरसञ्चार ऐन, २०५३, सूचनाको हक सम्बन्धी ऐन, २०६४, रेडियो ऐन, २०१४, रेडियो ऐन, २०१८, चलचित्र (निर्माण प्रदर्शन तथा वितरण) ऐन, २०२६, राष्ट्रिय सूचना प्रविधी विकास समिति (गठन) आदेश, २०५८, सूचनाको हक कार्यान्वयन सम्बन्धी अनुगमन निर्देशिका, २०७६, डिजीटल नेपाल फ्रेमवर्क, २०७६, छापाखाना र प्रकाशन सम्बन्धी नियमावली, २०४९, दुरसञ्चार नियमावली, २०५४ चलचित्र निर्माण प्रदर्शन तथा वितरण) नियमावली, २०६५ लगायतका ऐन तथा नियमावलीहरूमा प्रत्यक्ष तथा अप्रत्यक्ष रूपमा कम्प्युटरको प्रयोग गरी साइबर क्षेत्रमा हुने कसूरहरू नियन्त्रणको विषयलाई उल्लेख गरिएको छ।

४.१.३. नीतिगत व्यवस्था (Policy Provision)

नेपालमा पहिलो पटक २०२८ सालमा नेपाल जनगणनाको तथ्याङ्ढ प्रशोधनका क्रममा कम्प्युटर प्रविधिको प्रयोग भएको हो। २०३१ सालमा कम्प्युटरसँग सम्बन्धित पहिलो संस्था सेन्टर फर इलेक्ट्रोनिक डाटा प्रोसेसिङ स्थापना भयो जसको नाम पछि राष्ट्रिय कम्प्युटर केन्द्र भएको हो। राष्ट्रिय सञ्चार नीति २०४९, दूरसञ्चार ऐन, २०५३ र दूरसञ्चार नियमावली, २०५४ लागु भएपश्चात मुलुकमा दूरसञ्चार क्षेत्र खुला एवम् प्रतिस्पर्धी युगमा प्रवेश गरेको हो। २०५७ सालमा लागु भएको सूचना प्रविधि नीतिले सूचना प्रविधिलाई देश विकासको बृहत्तर लक्ष्य हासिल गर्ने औजारका रूपमा स्थापित गर्ने अवधारणा अघि सारेको थियो।

त्यसैगरी सूचना प्रविधिको उपयोगबाट सामाजिक एवम् आर्थिक विकासका लक्ष्यहरू हासिल गर्दै गरिबी न्यूनीकरण गर्ने लक्ष्यका साथ सूचना प्रविधि नीति, २०६७ जारी गरियो। उक्त नीतिमा प्रविधि प्रयोगमा सूचनाको सुरक्षा एवम् तथ्याङ्ढको गोपनीयतालाई सुदृढ गरिने विषयमा जोड दिइएको थियो।

नवौँ योजना (२०५४–२०५९) मा विद्यालयहरूमा कम्प्युटर शिक्षा व्यापकरूपमा विस्तार गर्ने, उच्च अध्ययनका लागि औपचारिक शिक्षा तथा उच्च तालिम व्यवस्था गर्ने, स्तरीय विद्यालय र सूचना प्रविधि पार्क स्थापना गर्ने र सरकारी कार्यालयमा योजना तर्जुमा र व्यवस्थापनमा कम्प्युटर उपयोगमा जोड दिनेलगायतका नीति कार्यक्रम थियो। तर योजना अवधिमा सूचना प्रविधि शिक्षाको विकास र विस्तारका लागि ४ वटा विश्वविद्यालयलाई अनुदान सहयोग उपलब्ध गराइएको, सूचना प्रविधि नीति, २०५७ जारी गरिएको र विद्युतीय कारोबार ऐन, नियम तयार गरिएको तथा बनेपामा सूचना प्रविधि पार्कको निर्माण सुरु गरिएको पाइन्छ। राष्ट्रिय आवश्यकताअनुसार सूचना प्रविधिको विकास र विस्तार गरी त्यसमा सर्वसाधारण जनताको सहज र सरल पहुँच सुनिश्चित गर्ने तथा राष्ट्रिय विकासमा सूचना प्रविधिको उच्चतम

उपयोग गर्ने राज्यको नीति छ।

विद्युतीय तथ्याङ्ढ आदान–प्रदानको माध्यमबाट वा अन्य कुनै विद्युतीय सञ्चार माध्यमबाट हुने कारोबारलाई भरपर्दो र सुरक्षित बनाइ विद्युतीय अभिलेख सिर्जना, उत्पादन, प्रशोधन, सञ्चय, प्रवाह तथा सम्प्रेषण प्रणालीको मान्यता, सत्यता, अखण्डता र विश्वसनीयतालाई प्रमाणीकरण तथा नियमित गर्ने व्यवस्था गर्न र विद्युतीय अभिलेखलाई अनधिकृततवरबाट प्रयोग गर्न वा त्यस्तो अभिलेखमा गैरकानुनीतवरबाट परिवर्तन गर्ने कार्यलाई नियन्त्रण गर्नका लागिघ पहिलो कानुनीरूपमा विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ तथा विद्युतीय कारोबार नियमावली, २०६४ कार्यान्वयनमा छन्।

सूचना तथा सञ्चार प्रविधिको प्रयोगबाट सुशासन प्रबद्र्धन गर्नेलगायतका उद्देश्य राखी सूचना तथा सञ्चार प्रविधि नीति, २०७२ जारी भई कार्यान्वयनमा छ। यस नीतिमा साइबर सुरक्षाको विषयलाई सम्बोधन गर्दै साइबर सुरक्षा निकाय स्थापना तथा साइबर आक्रमणको पहिचान, रोकथाम, प्रतिरक्षालगायतका आयामहरूको प्रभावकारीरूपमा सम्बोधन गर्ने, साइबर सुरक्षासम्बन्धी क्षमता अभिवृद्धि कार्यक्रम सञ्चालन गर्ने, आपत्कालीन कम्प्युटर उद्धार समूह स्थापना गरी साइबर सुरक्षासम्बन्धी चुनौतीहरू शीघ्र सम्बोधन गर्ने व्यवस्था मिलाइने उल्लेख छ।

राष्ट्रिय सुरक्षा नीति, २०७५ ले साइबर सुरक्षालाई राष्ट्रिय सुरक्षाको एक महत्वपूर्ण आयामका रूपमा समेटेको छ। सूचना प्रविधिको विकास तथा बढ्दो प्रयोगसँगै देखिएको साइबर सुरक्षा जोखिमको पहिचान, त्यसबाट हुने असरको न्यूनीकरण र आकस्मिक साइबर सुरक्षाको व्यवस्था गर्ने उद्देश्यले सूचना प्रविधि आकस्मिक सहायता समूह सञ्चालन तथा व्यवस्थापन निर्देशिका, २०७५ जारी भई कार्यान्वयनमा छ। उक्त निर्देशिकामा व्यवस्था भएअनुरूप राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूह र राष्ट्रिय साइबर सुरक्षा अनुगमन केन्द्र स्थापना भइ सरकारी सूचना प्रविधि प्रणालीहरूको निरन्तर अनुगमन भइरहेको छ।

चालु आवधिक योजनाले साइबर सुरक्षा तथा गोपनीयतासम्बन्धी कार्य गर्न साइबर सुरक्षा अनुगमन केन्द्र स्थापना गरी साइबर सुरक्षालाई प्रभावकारी बनाइने विषयलाई जोड दिएको छ। डिजिटल नेपाल फ्रेमवर्क, नेपाल २०७६ मा राष्ट्रिय साइबर सुरक्षा केन्द्र स्थापनालगायतका साइबर सुरक्षासँग सम्बन्धित विषयहरूलाई समावेश गरिएको छ। दूरसञ्चार तथा इनटरनेट सेवा प्रदायकहरूको सूचना प्रविधि प्रणाली समेटिने गरी साइबर सुरक्षा विनियमावली, २०७७ कार्यान्वयनमा छ। सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिका, २०७१ साथै अनलाइन बाल सुरक्षा निर्देशिका, २०७६ कार्यान्वयनमा छन्।

१. राष्ट्रिय साइबर सुरक्षा नीति, २०८०

नेपाल सरकारको वार्षिक नीति तथा कार्यक्रममा साइबर सुरक्षासम्बन्धी विषयलाई प्राथमिकताका साथ उल्लेख गरेको पाइन्छ। राष्ट्रिय साइबर सुरक्षा नीति, २०८० ले उठान गरेका विषय नेपालको सन्दर्भमा राष्ट्रिय साइबर सुरक्षा नीतिका रूपमा पारित भएको यो पहिलो साइबर सुरक्षा नीति हो। यसले आगामी दिनमा साइबर सुरक्षा सम्बन्धमा निर्माण हुने कानुनहरूका सन्दर्भमा मार्ग निर्देशकका रूपमा काम गर्छ।

हाल जारी राष्ट्रिय साइबर सुरक्षा नीति, २०८० को सन्दर्भमा व्यापकरूपमा छलफल गरी यसमा भएका कमजोरी औल्याएको खण्डमा आगामी दिनमा कानुन निर्माणका सन्दर्भमा यो नीतिले सार्थकता पाउन सक्छ। नेपालको सन्दर्भमा साइबर सुरक्षाका लागि प्रभावकारी कानूनी व्यवस्था तथा संस्थागत संरचना नहुनु, साइबर सुरक्षासम्बन्धी

भौतिक तथा प्राविधिक पूर्वाधारको कमी, साइबर सुरक्षाका क्षेत्रमा दक्ष जनशक्ति तथा अनुसन्धानको कमी, साइबर सुरक्षासम्बन्धी सचेतनाको कमी, साइबर सुरक्षा सम्बन्धमा आन्तरिक तथा बाह्य समन्वयमा कमी जस्ता पक्षलाई समस्याका रूपमा राष्ट्रिय साइबर सुरक्षा नीतिले उल्लेख गरेको छ।

यसका साथै सूचना तथा सञ्चार प्रविधि प्रणालीमा हुने साइबर आक्रमणको जोखिम न्यून गर्नका लागि नीतिगत र संरचनागत व्यवस्था गर्नु, साइबर सुरक्षा सुनिश्चित गर्न समयानुकूल अनुसन्धान र क्षमतामा आधारित दक्ष जनशक्ति विकास र उपयोग गर्नु, राष्ट्रिय संवेदनशील पूर्वाधार को पहिचान एवम् संरक्षण गर्नु, सार्वजनिक, व्यावसायिक र व्यक्तिगत सूचना तथा तथ्याङ्कमा अनधिकृत पहुँच नियन्त्रण गर्नु, नागरिक सेवामा विश्वसनीय डिजिटल प्रणाली र साइबर सुरक्षा प्रत्याभूत गर्नु, साइबर सुरक्षाका लागि राष्ट्रिय तथा अन्तर्राष्ट्रिय सहयोग तथा समन्वय गर्नुलाई नीतिले प्रमुख चुनौतीका रूपमा औल्याएको छ। सञ्चार प्रविधिको प्रयोगलाई अझ सशक्तीकरण गर्दै सूचना तथा सञ्चार प्रविधि सम्बन्धमा जारी क्रियाकलापहरूलाई सम्बोधन गर्नका लागि राष्ट्रिय सूचना तथा सञ्चार प्रविधि नीतिका अतिरिक्त राष्ट्रिय साइबर सुरक्षा नीतिलाई पनि अपनाउने निर्णय भएको पाइन्छ। यस नीतिले मूलतः मौजुदा नीतिहरूमा आधार भई निर्माण भएको र सूचना तथा सञ्चार प्रविधिको प्रयोगमा बचाव र सुरक्षा (Safety & Security) को वृद्धि गर्न यसले लक्ष्य तथा उद्देश्यहरूको तर्जुमा गरेको छ। यसका अतिरिक्त यसले सहस्राब्दी विकास लक्ष्य (Millennium Development Goals) का उद्देश्यहरू, अन्तर्राष्ट्रिय दूरसञ्चार सम्मेलन बुसान,२०१४ (Final Acts of the ITU Plenipotentiary Conference Busan, २०१४) तथा अन्तर्राष्ट्रिय दूरसञ्चार संघ (ITU) बाट पारित सिफारिसहरूलाई प्रतिबिम्ब गरेको छ। यस नीतिले साइबर सुरक्षाका लागि प्राविधिक निर्देशिका (Technical Guidelines) एवम् राष्ट्रिय साइबर सुरक्षा रणनीतिको अन्य प्राविधिक तथा संगठनात्मक अङ्गहरूको विकास गर्ने लक्ष्य लिएको पाइन्छ। अन्य लक्ष्यहरूमा केही महत्त्वपूर्ण लक्ष्यहरू यस प्रकार रहेका छन्:--

- राष्ट्रिय कम्प्युटर आपतकालीन पहल टोली (Nepal Computer Emergency Response Team) को स्थापनालगायतका अन्य संगठनात्मक संरचनाहरूलाई ससक्त बनाउने।
- सरोकारवालाहरू बिच आवश्यक सूचनाको निरन्तर आदन प्रदान गर्न दिने वातावरणको सिर्जना गर्ने।
- संवेदनशील आधारभूत पूर्वाधारसँग सम्बन्धित साइबर जोखिमको सुरक्षालाई सवलीकरण गरिने छ।
- अपराधिकरण, अनुसन्धान, विद्युतीय प्रमाण तथा अन्तर्राष्ट्रिय सहयोगका साथै मौलिक अधिकारहरूको संरक्षणका सन्दर्भमा उच्चतम क्षेत्रीय एवम् अन्तर्राष्ट्रिय मापदण्ड/स्तर कायम गर्न नेपालको कानूनी तथा नीतिगत व्यवस्थालाई सशक्त बनाइने |

यस नीतिले साइबर सुरक्षा रणनीतिक कार्यसमूह (National Cyber Security Strategy Working Group-NCSWG) को परिकल्पना गरी सोद्वारा साइबर सुरक्षा नीति तयार गरी सोद्वारा निम्न विषयहरूको सम्बोधन गर्ने व्यवस्था मिलाएको छ।

- सरकारी र निजी क्षेत्रको जिम्मेवारी
- जोखिम निर्धारण र आपत्कालीन योजनाहरू
- यसका अलवा बाल अनलाइन सुरक्षा (Child Online Protection)

- संवेदनशील पूर्वाधार सुरक्षा र यसको वर्गीकरण
- राष्ट्रिय सूचना तथा सञ्चार प्रविधि गुरूयोजना
- राष्ट्रिय विद्युतीय रणनीतिको स्थापना

२. सूचना तथा सञ्चार प्रविधि नीति, २०७२

विद्युतीय व्यापार (e-Commerce), विद्युतीय सरकार (e- Government) मा जोड, इन्टरनेट सेवा सहितका सूचना केन्द्रको विस्तार गर्ने, ग्रामीण दूर सञ्चार विकास कोष परिचालन, e-School, e- learning, e-education मा जोड, Software & Services Promotion Board को स्थापना गर्ने, (Payment Infrastructure Services) हरूको स्थापना, टेलिमेडिसिन योजना तर्जुमा, स्मार्ट सिटी (smart city) को अवधारणा अघि सारिएको हो।

४.२. नेपालमा साइवर कसूरको नियन्त्रण र सम्बोधनको लागि भएका संस्थागत तथा पद्धतीगत व्यवस्था (Institutional Mechanism for Controlling Cyber Crime in Nepal)

नेपालमा साइवर कसूरको नियन्त्रण र सम्बोधनको लागि भएका संस्थागत तथा पद्धतीगत प्रयासहरू यस प्रकार रहेको छ।

(१) साइबरसंग सम्बन्धित कसूरको विशिष्टिकृत अनुसन्धान तहकिकात गर्न, साइबरसँग सम्बन्धित कसूर न्यूनिकरण गर्न र प्रहरी कार्यालयबाट भइरहेको वा हुने साइबरसंग सम्बन्धित कसूरहरूको अनुसन्धान, तहकिकातका कार्यमा आवश्यक सहयोग, समन्वय गर्न, निर्देशन दिन, साइबर सुरक्षा तथा सचेतनाका कार्यक्रम संचालनका निमित्त नेपाल सरकारको मिति २०७५।२।२४ को निर्णय बमोजिम प्रहरी प्रधान कार्यालय अन्तर्गत केन्द्रीय साइबर ब्यूरोको स्थापना गरी कृयाशिल रहेको छ।

(२) सरकारी निकायहरूले वेबसाईट निर्माण गरी विभिन्न गतिविधि तथा सूचनाहरूलाई व्यवस्थित गर्ने गरेको देखिन्छ।

(३) केन्द्रीय तहका सरकारी निकायहरूमा सूचना प्रविधि तथा विद्युतीय सुशासन शाखाको स्थापना गरी सञ्चालनमा आएको छ।

(४) इन्टरनेट सोसाइटी नेपालको स्थापना भई कृयाशिल रहेको छ।

(५) अभियोजनको क्रममा पीडितको वा प्रतिवादीको रूपमा नाबालक रहेको अवस्थामा नाम, थर, वतन परिवर्तन गरेर गोपनीयता कायम गर्ने गरिएको छ।

(६) प्रहरी प्रधान कार्यालयमा सन् २०१५ देखि Digital Forensic Lab को स्थापना गरी प्रयोगमा ल्याइएको छ।

(७) महान्यायाधीवक्ताको कार्यालयमा सरकारी वकिलहरूको लागि साइबर कसूर सम्बन्धी विशिष्टिकृत प्रशिक्षणको शुरूवात भएको छ।

(८) सेवा प्रवेश तथा सेवा कालीन तालिममा प्रशिक्षणको लागि साइवर कसूरको विषयलाई समावेश गर्ने गरिएको छ।

परिच्छेद पाँच

सर्वोच्च अदालतबाट प्रतिपादित नजिर तथा निर्देशनको विश्लेषण

५.१ न्यायिक दृष्टिकोण (Judicial Approach)

साइबर कसूरको सम्बन्धमा सर्वोच्च अदालतबाट प्रतिपादित नजिर सिद्धान्तलाई यहाँ प्रस्तुत गरिएको छ।

१. **रामप्रताप खड्का विरूद्ध महानगरीय प्रहरी परिसर:**[१] कोहीनुर नामक चलचित्र गैरकानूनीरूपमा इन्टरनेटमा अपलोड गरी विद्युतीय कारोबार ऐन, २०६३ र प्रतिलिपि अधिकार ऐन, २०५९ को प्रतिकूलको कसुर भएको भनि दिएको जाहेरी दरखास्त महानगरीय प्रहरी परिसर काठमाडौंले दर्ता नगरेको हुँदा जाहेरी दरखास्त दर्ता गरी रीतपूर्वक अनुसन्धान गरी पाउँ भन्ने माग दावी भएको प्रस्तुत रीटमा परमादेशको आदेश जारी गरी निम्न सिद्धान्त प्रतिपादन गरेको छ।

अनधिकृतरूपमा विभिन्न वेबसाइटहरूमा राखिएका कोहिनुर चलचित्र नरोक्ने हो भने चलचित्र निर्मातालाई अपूरणीय क्षतिसमेत हुन जाने देखिएकाले नेपाल विद्युतीय कारोबार ऐन, २०६३ को दफा ४४, ४५, ४६ र ४७ तथा प्रतिलिपि अधिकार ऐन, २०५९ को दफा २५ विपरीतको कसुरमा यस ऐनबमोजिम सरकारी मुद्दा सम्बन्धी ऐन, २०४९ को दफा ३ बमोजिम निवेदकको जाहेरी दरखास्त दर्ता गरी कोहीनुर चलचित्रको अनाधिकृतरूपमा विभिन्न वेबसाइटमा अपलोड गरी प्रदर्शन राखिएको कार्यका सम्बन्धमा जो जसले गरेको भए तापनि अनुसन्धान गरी कारवाहीको प्रक्रिया अगाडि बढाउन निवेदकको उजुरी दर्ता गरी अनुसन्धान गरी उक्त आपराधिक कार्य पत्ता लगाई रोक्ने कार्यसमेत गर्नु भनी विपक्षीहरूको नाउँमा परमादेशको आदेश जारी हुने भनी ब्याख्या भएको छ।

२. **ख कुमारीको जाहेरीले नेपाल सरकार विरूद्ध प्रकाश ओझा:**[२] जिउ मास्ने बेच्ने सम्बन्धमा दायर भएको प्रस्तुत मुद्दा साइबर कसूरसँग प्रत्यक्ष रूपमा सम्बन्धित रहेको नभएता पनि यस मुद्दामा प्रतिपादित सिद्धान्त साइबर कसूरको स्वरूप अन्तर्गत रहेको Pornography विरूद्ध पनि लक्षित रहेको भने मान्न सकिन्छ। प्रतिवादी प्रकाश ओझाले अनुचित प्रभावमा पारी पीडितसँग शारीरिक सम्पर्क राख्ने, चलचित्र खिच्ने तथा स्त्री जातिको यौन अंगको प्रर्दशन गरी आर्थिक लाभ लिनको लागि गरेको कार्य जिउ मास्ने बेच्ने कार्य नियन्त्रण ऐन, २०४३ को दफा ४ को खण्ड (ग) द्वारा निषेधित कसुर हुँदा सजाय गरिपाउँ भनी अभियोगपत्र दायर भएकोमा प्रतिवादीले अभियोगदाबीबाट सफाई पाउने ठहर्‌याई भएको जिल्ला अदालतको फैसलालाई पुनरावेदन अदालत बाट सदर गरेकोमा दोहोर्‌याइ हेर्ने निस्सा दिइ सर्वोच्च अदालतबाट उल्टी गरी निम्न सिद्धान्त प्रतिपादन गरेको छ।

पीडितसमेतको तस्वीर संग्रहित चिप्स हराउँदा प्रतिवादी चिन्तित रहेका सो चिन्तालाई निजले व्यक्त गरेका र खिचेका तस्वीरहरू नष्ट गर्न पनि लोभ लागेको थियो भनी प्रतिवादीको मौकाको बयानमा उल्लेख भएको व्यहोरासमेतबाट यौनक्रीडारत अवस्थामा तथा स्त्री अङ्गहरू प्रदर्शन गर्ने गरी फोटो खिच्नु पर्ने र त्यसलाई चिनी क्यामराको चिप्समा संग्रह गरी राख्नुपर्नेसम्मको कारण निजले खुलाउन सकेको पाइँदैन। यी दृश्यहरू व्यक्तिगत

१ निर्णय नं. ९४३५ परमादेश

२ निर्णय नं. ९६२१ - जिउ मास्ने बेच्ने

प्रयोजनमा आउन नसक्ने प्रकृतिका देखिँदा आफूसँग यौन सम्पर्क राखी खिचेको फोटाबाट अश्लील चलचित्र बनाई बिक्री गर्ने प्रतिवादीको योजना रहेको, अनुचित प्रभावमा पारी पीडितसँग शारीरिक सम्पर्क राख्ने, चलचित्र खिच्ने तथा स्त्री जातिको यौन अंगको प्रर्दशन गरी आर्थिक लाभ लिनको लागि गरेको कार्यलाई वेश्यावृत्तिमा लगाएको मान्नुपर्ने हुन्छ भनी अभियोगपत्रमा उल्लेख भएको व्यहोरा बडो तार्किक छ । नाबालकसमेतको नग्न तस्वीर खिचेको लाई समेत तल्ला अदालतले कानून छैन भनेर गरेको फैसलाले पीडितको पीडालाई अनुभूत गरेको देखिएन । कानून र न्यायलाई असहाय बनाएको देखियो । कानून र न्याय कहिल्यै असहाय हुँदैनन् । त्यसलाई जीवन्त बनाउने न्यायाधीश असहाय भएमा मात्र कानून र न्याय असहाय हुन पुग्न देखिन आउने भनी व्याख्या भएको छ ।

परिच्छेद छ

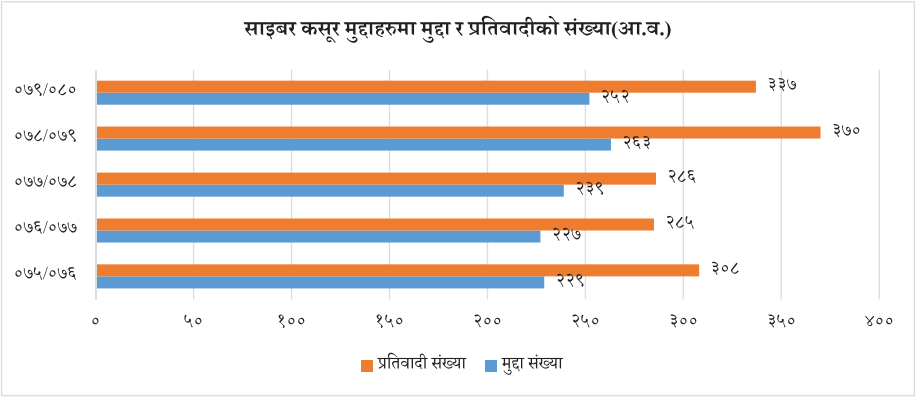
संकलित सूचना/तथ्याङ्क र सोको विश्लेषण

६.१ नेपालमा साइबर कसूरको अनुसन्धान र अभियोजन सम्बन्धी व्यवस्था (Provision of Investigation and Prosecution of Cyber Crime)

साइबर कसूरको अनुसन्धान र अभियोजनको सम्बन्धमा विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ को दफा ७५ मा उल्लिखित दफा आकर्षित हुन्छ । यस दफामा यस ऐन बमोजिम कसूर ठहर्ने मुद्दा नेपाल सरकार वादी भई चल्ने र त्यस्तो मुद्दा अनुसूची–१ मा समावेश भएको मानिनेछ तथा यस्तो मुद्दामा अनुसन्धान गर्दा प्रहरीले नियन्त्रक वा अन्य सम्बन्धित विशेषज्ञको सहयोग लिनु पर्ने भन्ने उल्लेख छ । प्रहरी प्रधान कार्यालयमा रहेको केन्द्रिय साइबर ब्युरोबाट साइबर कसूर सम्बन्धमा अनुसन्धान गर्ने कार्य गर्दछ । प्रहरी नायब महानिरीक्षक (डीआईजी) ले नेतृत्व गर्ने यस ब्यूरोले देशभर हुने साइबर सम्बन्धी कसूरको अनुसन्धान गर्ने गर्छ । काठमाडौंको उपत्यकाबाहिरको हकमा सीआईबी र काठमाडौं उपत्यकाको हकमा महानगरीय प्रहरी कसूर महाशाखाले साइबर सम्बन्धी कसूरको अनुसन्धान गर्ने गरेको छ । साइबर ब्यूरोले सात वटै प्रदेश प्रहरी कार्यालयमा साइबर सेल स्थापना गरिसकेको छ । ती सेलले प्रदेश भरका साइबर सम्बन्धी कसूरको अनुसन्धान गर्दछन् । अनुसन्धान पश्चात् जिल्ला अदालतमा सम्बन्धित सरकारी वकिलबाट अभियोजनको कार्य हुन्छ । यसरी साइबर कसूरको अनुसन्धान नेपाल प्रहरीबाट र अभियोजनको कार्य भने सम्बन्धित सरकारी वकिलमार्फत हुदै आएको छ ।

६.२. विद्युतीय कारोबार सम्बन्धी मुद्दाको अभियोजन र फैसला सम्बन्धी रहेको अद्यावधिक विवरण

तालिका १

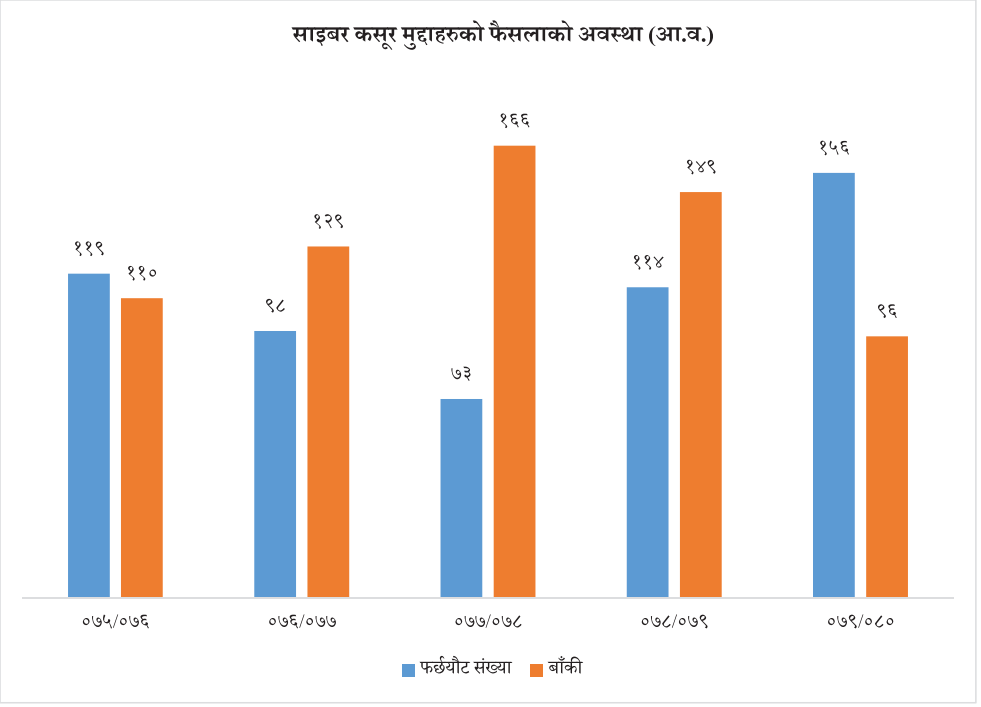


स्रोतः महान्यायाधिवक्ताको कार्यालयको वार्षिक प्रतिवेदनहरु

माथि प्रस्तुत तालिका अनुरूप आ.व. २०७५ । ०७६ मा विद्युतीय कारोबार सम्बन्धी कुल २५२ मुद्दामा ३३७ प्रतिवादीहरु रहेको देखिन्छ । यसैगरी, आ.व. २०७६ । ०७७ मा विद्युतीय कारोबार सम्बन्धी कुल २६३ मुद्दामा ३७०

प्रतिवादीहरु रहेको देखिन्छ, आ.व. २०७७।०७८ मा विद्युतीय कारोबार सम्बन्धी कुल २३९ मुद्दामा २८६ प्रतिवादीहरु रहेको देखिन्छ भने आ.व. २०७८।०७९ मा विद्युतीय कारोबार सम्बन्धी कुल २२७ मुद्दामा २८५ प्रतिवादीहरु रहेको देखिन्छ र आ.व. २०७९।०८० मा विद्युतीय कारोबार सम्बन्धी कुल २२९ मुद्दामा ३०८ प्रतिवादीहरु रहेको देखिन्छ।

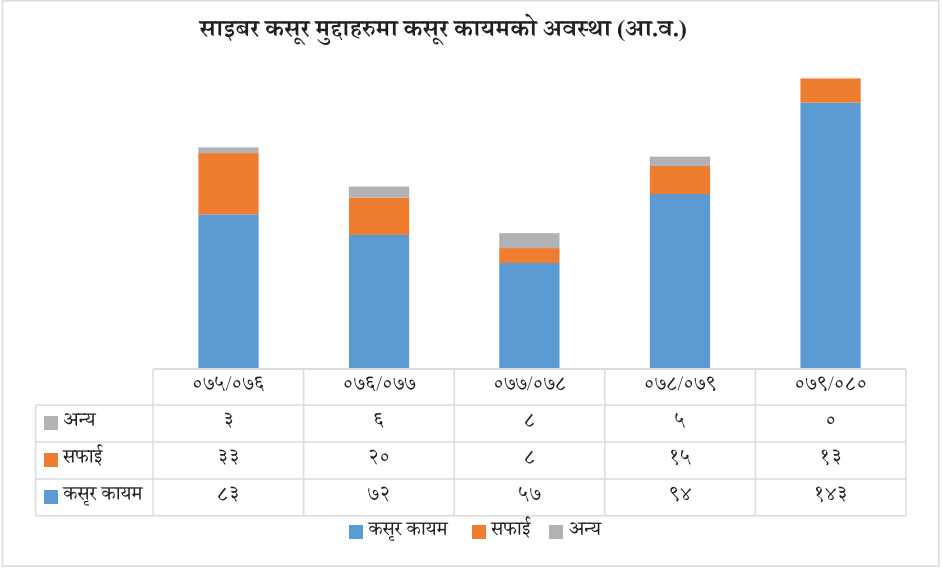
तालिका २



स्रोतः महान्यायाधिवक्ताको कार्यालयको वार्षिक प्रतिवेदनहरु

माथि प्रस्तुत तालिका अनुरूप आ.व. २०७५।०७६ मा साइबर कसूर सम्बन्धी कुल ११९ वटा मुद्दाहरु फछ्यौंट भएको देखिएकोमा उक्त आ.व. मा ११० वटा मुद्दा बाँकी रहेको देखियो। यसैगरी, आ.व. २०७६।०७७ मा साइबर कसूर सम्बन्धी कुल ९८ वटा मुद्दाहरु फछ्यौंट भएको देखिएकोमा उक्त आ.व. मा १२९ वटा मुद्दा बाँकी रहेको देखियो, आ.व. २०७७।०७८ मा साइबर कसूर सम्बन्धी कुल ७३ वटा मुद्दाहरु फछ्यौंट भएको देखिएकोमा उक्त आ.व. मा १६६ वटा मुद्दा बाँकी रहेको देखियो, आ.व. २०७८।०७९ मा साइबर कसूर सम्बन्धी कुल ११४ वटा मुद्दाहरु फछ्यौंट भएको देखिएकोमा उक्त आ.व. मा १४९ वटा मुद्दा बाँकी रहेको देखियो र आ.व. २०७९।०८० मा साइबर कसूर सम्बन्धी कुल १५६ वटा मुद्दाहरु फछ्यौंट भएको देखिएकोमा उक्त आ.व. मा ९६ वटा मुद्दा बाँकी रहेको देखियो। यसरी ५ मध्ये ३ वटा आ.व. मा मुद्दा फछ्यौंट भन्दा बाँकी रहेको मुद्दाको संख्या धेरै रहेको देखिन्छ। आ.व. २०७५।०७६ मा ११९ वटा मुद्दा फछ्यौंट भएको देखिएकोमा आ.व. २०७९।०८० मा सबै भन्दा धेरै १५६ वटा मुद्दा फछ्यौंट भएको देखिन्छ। सबै भन्दा कम मुद्दा आ.व. २०७७।०७८ मा फछ्यौंट भएको देखिन्छ।

तालिका ३

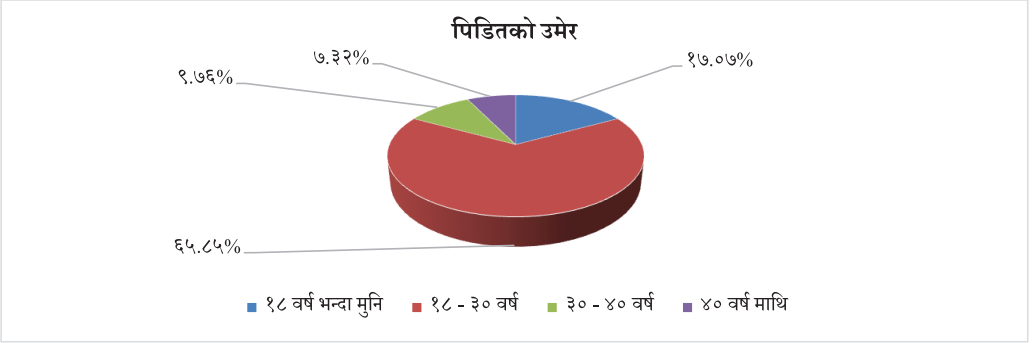


स्रोतः महान्यायाधिवक्ताको कार्यालयको वार्षिक प्रतिवेदनहरु

माथि प्रस्तुत तालिका अनुरूप आ.व. २०७५।०७६ मा विद्युतीय कारोबार सम्बन्धी ८३ मुद्दामा कसूर कायम भएको देखिन्छ भने ३३ वटामा सफाई भएको देखिन्छ साथै, ३ वटा मुद्दामा अन्य कारवाही भएको देखिन्छ। यसैगरी, आ.व. २०७६।०७७ मा विद्युतीय कारोबार सम्बन्धी ७२ मुद्दामा कसूर कायम भएको देखिन्छ भने २० वटामा सफाई भएको देखिन्छ साथै, ६ वटा मुद्दामा अन्य कारवाही भएको देखिन्छ, आ.व. २०७७। ०७८ मा विद्युतीय कारोबार सम्बन्धी ५७ मुद्दामा कसूर कायम भएको देखिन्छ भने ८ वटामा सफाई भएको देखिन्छ साथै, ८ वटा मुद्दामा अन्य कारवाही भएको देखिन्छ, आ.व. २०७८। ०७९ मा विद्युतीय कारोबार सम्बन्धी ९५ मुद्दामा कसूर कायम भएको देखिन्छ भने १५ वटामा सफाई भएको देखिन्छ साथै, ५ वटा मुद्दामा अन्य कारवाही भएको देखिन्छ र आ.व. २०७९। ०८० मा विद्युतीय कारोबार सम्बन्धी १४३ मुद्दामा कसूर कायम भएको देखिन्छ भने १३ वटामा सफाई भएको देखिन्छ। यसरी समग्रमा विद्युतिय कारोबार सम्बन्धी मुद्दामा सफलता दर वर्षै पिच्छे बढेको देखिन्छ। आ.व. २०७९।०८० मा ९०% हाराहारी मुद्दामा नेपाल सरकारलाई सफलता प्राप्त भएको देखिन्छ।

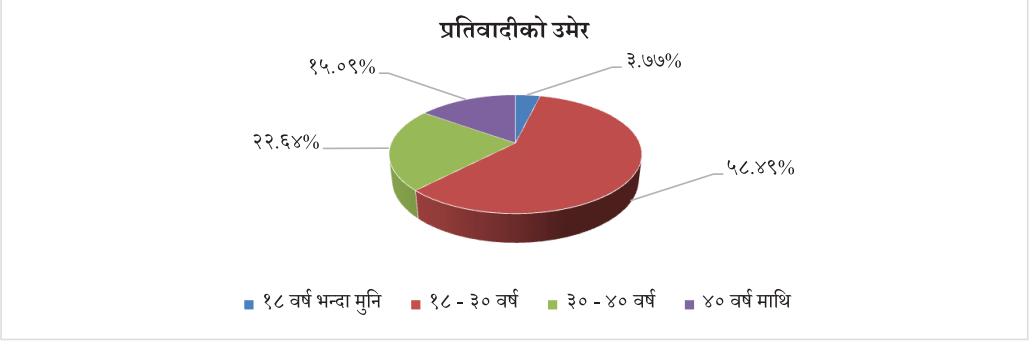
६.३. मिसिल अध्ययनबाट प्राप्त नतिजा

१. पीडितको उमेर



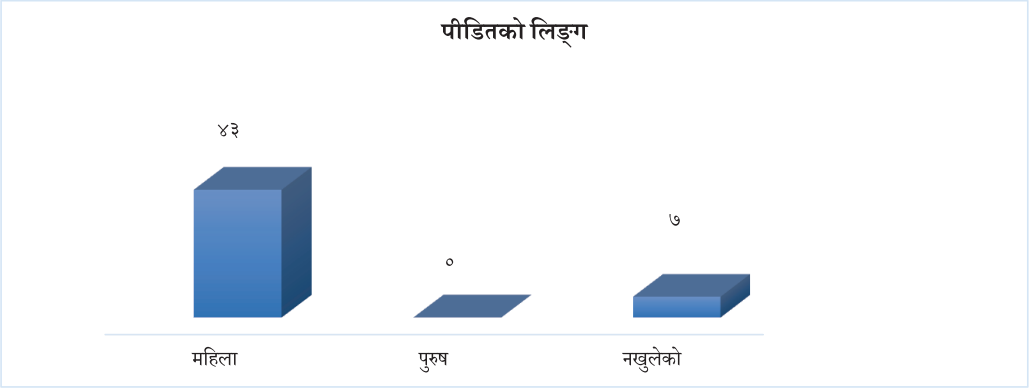
माथि प्रस्तुत बृतचित्रमा देखाए बमोजिम विद्युतीय कारोबार सम्बन्धि कसूरमा पीडित हुने व्यक्तिहरुको उमेर समूहको अनुपात अध्ययन गर्दा १८-३० वर्षका व्यक्तिहरुको सङ्ख्या जम्मा सङ्ख्याको ६५.८५% रहि सबै भन्दा बढी पीडित भएको देखियो । त्यसपछि १८ वर्ष मुनिका बालबालिकाको सङ्ख्या समेत उल्लेख्य रहेको (१७.०७%) देखियो । ३०-४० वर्ष उमेरका पीडित ९.७६% रहेको देखियो भने ४० वर्ष भन्दा माथीका व्यक्तिहरु समेत पीडित रहे तापनि अनुपात सबैभन्दा कम (७.३२%) रहेको पाईयो ।

२. प्रतिवादीको उमेर



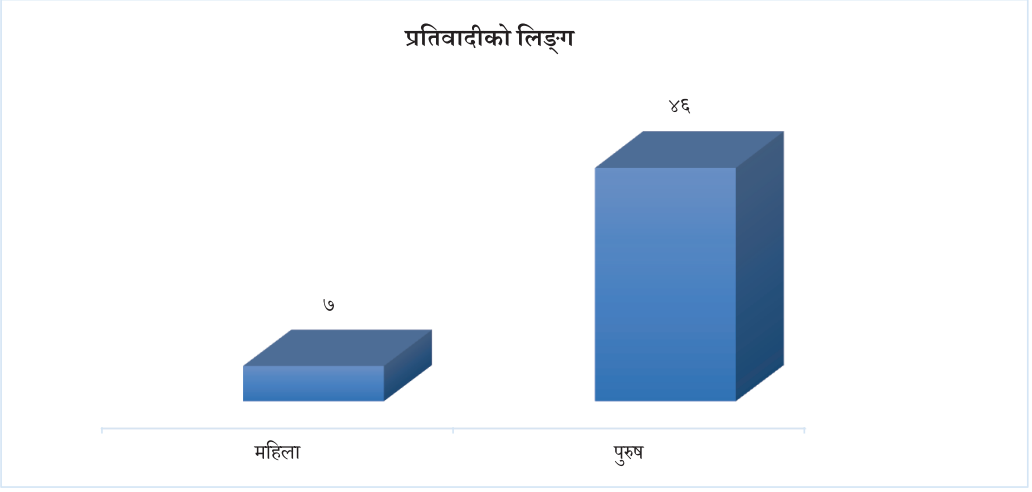
माथि प्रस्तुत बृतचित्रमा देखाए बमोजिम प्रतिवादीहरुको उमेर समूहको आधारमा निजहरुको संलग्नता अध्ययन गर्दा १८-३० वर्षको उमेर समूहका व्यक्तिको संलग्नता सबैभन्दा बढी रहेको (५८.४९%) पाईयो । ३०-४० वर्षको उमेरका व्यक्तिहरुको संख्या कुल प्रतिवादीमा २२.६४% रहेको र ४० वर्ष भन्दा माथीका व्यक्तिहरु सङ्ख्या १५.०९% रहेको देखियो । नाबालकहरुको समेत संलग्नता हुने गरेको तथ्याङ्कले देखाए तापनि उक्त सङ्ख्या न्यून रहेको (३.७७%) पाईयो ।

३. पीडितको लिङ्ग



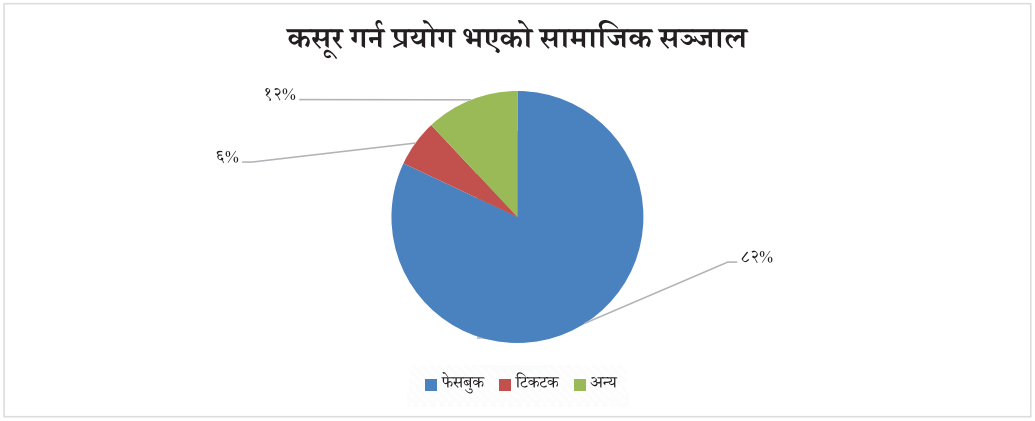
माथि प्रस्तुत बृतचित्रमा देखाए बमोजिम र अध्ययनबाट देखिए बमोजिम महिलाहरु नै विद्युतीय कारोबार सम्बन्धि कसूरको जोखिममा रहेको देखियो । कुल ५० जना पीडित मध्ये ४३ जना महिला र ७ जनाको हकमा प्रहरी प्रतिबेदनको आधारमा अनुसन्धान भएको कारण लिङ्ग नखुलेको अवस्थामा पाईयो ।

४. प्रतिवादीको लिङ्ग



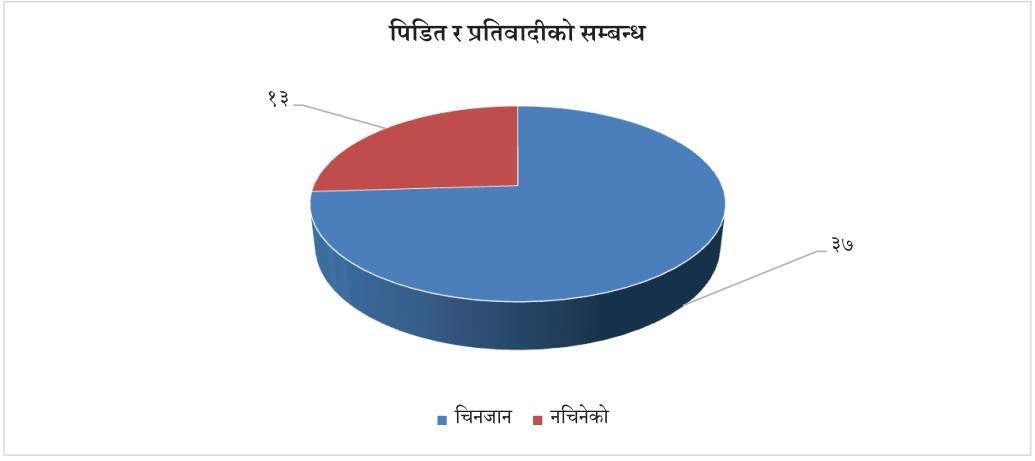
अध्ययन गरिएका मुद्दाहरुमा जम्मा ५३ जना प्रतिवादी रहेकोमा पुरुषको सङ्ख्या उल्लेख्य (४६ जना) रहि ७ जना महिला संलग्न रहेको पाईयो ।

५. कसूर गर्न प्रयोग भएको सामाजिक सञ्जाल



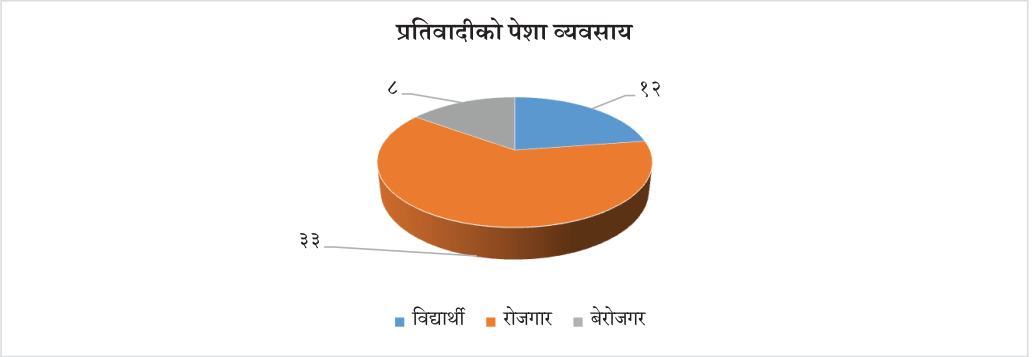
विद्युतीय कारोबार सम्बन्धि कसूर विशेषगरी सामाजिक सञ्जालको प्रयोगबाट भएको पाईएकोमा ८२% कसूर फेसबुकको प्रयोगबाट, ६% टिकटकको माध्यमबाट र बाँकी अन्य सञ्जालको प्रयोगबाट भएको देखियो।

६. पीडित र प्रतिवादीको सम्बन्ध



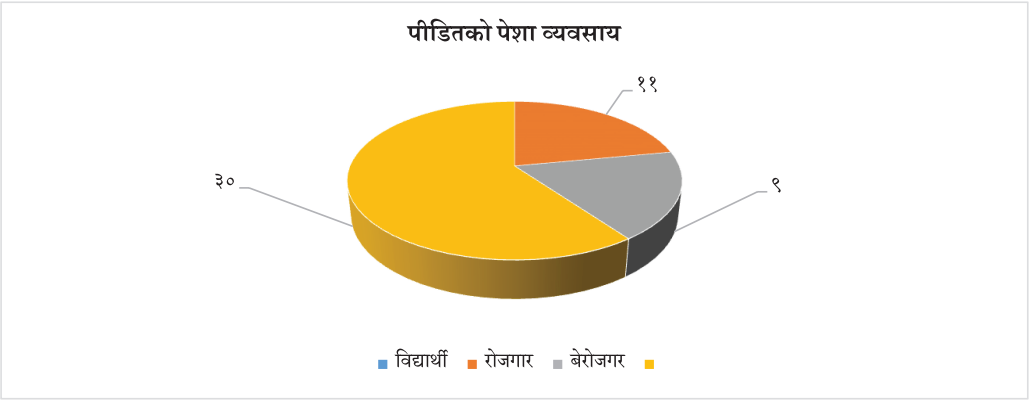
पीडित र प्रतिवादीबिचको सम्बन्ध अध्ययन गर्दा यस प्रकृतिको कसूरमा चिनजान रहेका व्यक्तिहरुबाट बढी जोखिम रहेको देखियो। ५० जना प्रतिवादीहरु मध्ये ३७ जना प्रतिवादीहरुसँग पीडितको पूर्व चिनजान रहेको पाईयो।

७. प्रतिवादीको पेशा व्यवसाय



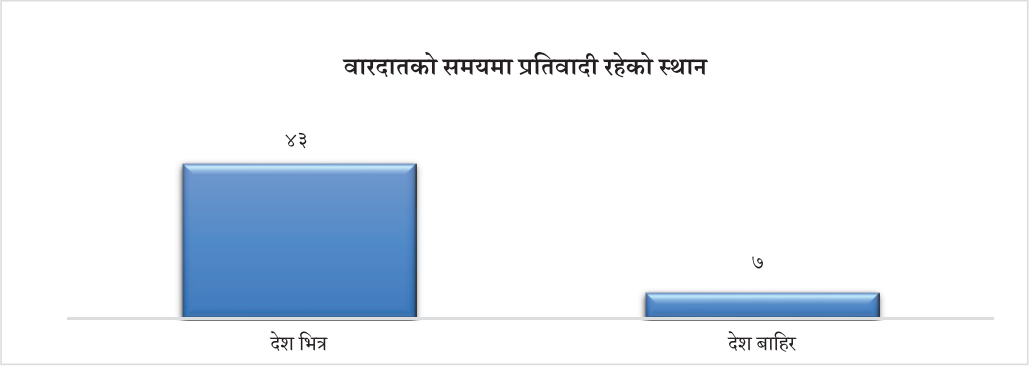
अध्ययनबाट पेशा व्यवसायमा लागेको व्यक्तिहरुबाट नै बढी कसूर हुने गरेको देखियो भने विद्यार्थीको एवम् बेरोजगार व्यक्तिहरुको संलग्नता तुलनात्मक हिसाबले कम देखियो। जम्मा ५३ प्रतिवादीमा ३३ जना कुनै पेशामा आवद्ध रहेको, १२ जना विद्यार्थी र ८ जना बेरोजगार व्यक्ति रहेको देख्न सकिन्छ।

८. पीडितको पेशा व्यवसाय



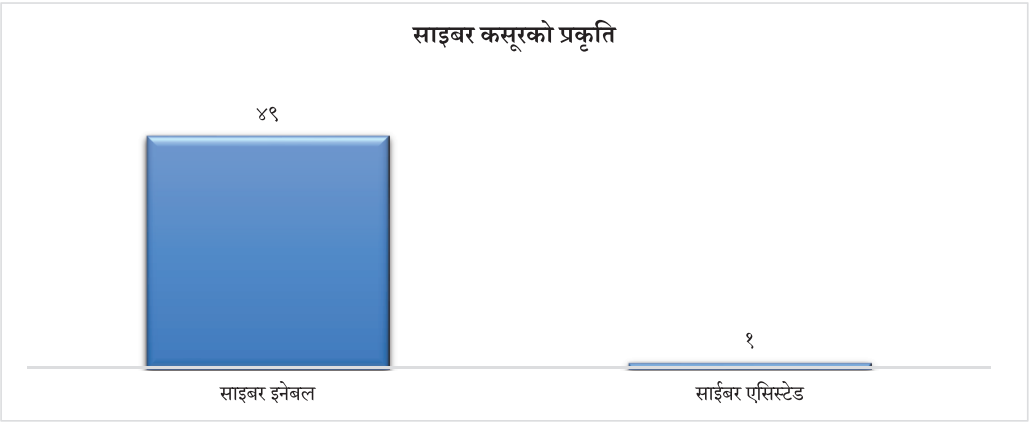
अध्ययनबाट पेशा व्यवसायमा आवद्ध नरहेका व्यक्तिहरु कसूरको बढी जोखिममा रहेको पाईयो। ५० जना पीडितहरु मध्ये ३० जना बेरोजगार, ९ जना रोजगार र ११ जना विद्यार्थी रहेको पाईयो।

९. वारदातको समयमा प्रतिवादी रहेको स्थान



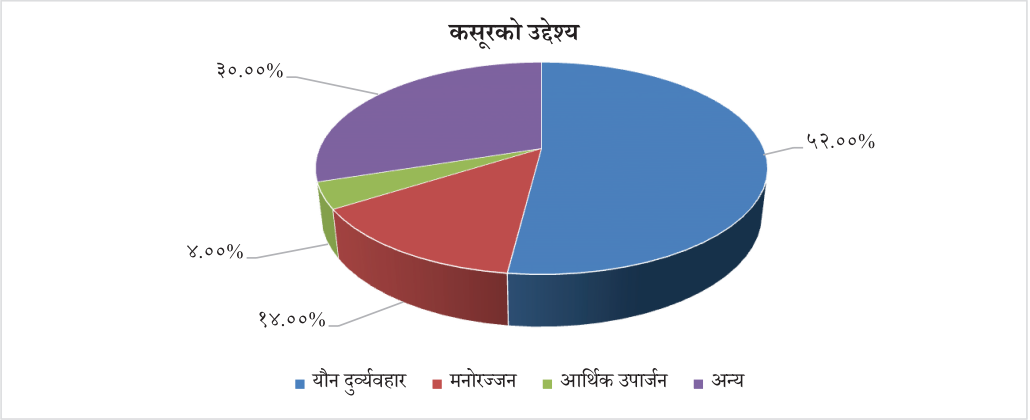
माथि प्रस्तुत तालिकाबाट प्रतिवादीहरुमा देशभित्र रहेर विद्युतीय कसूर गर्नेको सङ्ख्या उल्लेखनिय रुपमा बढी र देश बाहिरबाट गर्नेको सङ्ख्या तुलनात्मक रुपमा निकै कम पाईयो । अध्ययन गरिएका मुद्दाहरुका ५० जना प्रतिवादी मध्ये ४३ जना देश भित्र रहेको र ७ जना देश बाहिर रहेको देखियो ।

१०. साइबर कसूरको प्रकृति



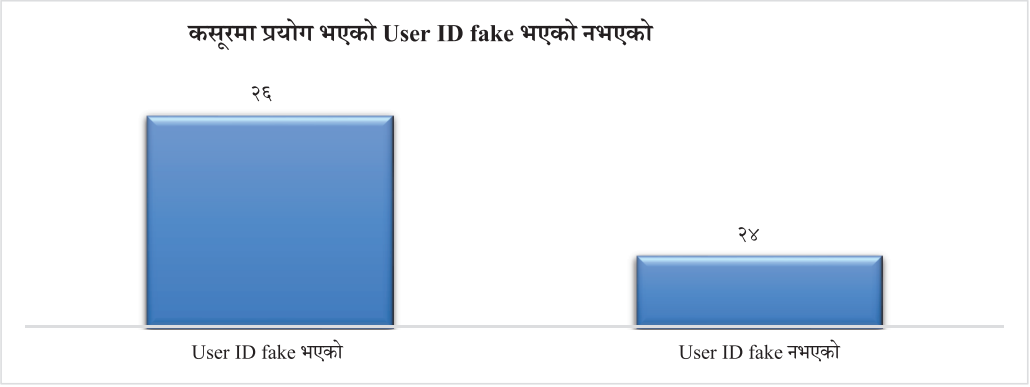
नेपालमा हुने साइबर कसूर मध्य साइबर इनेबल्ड (cyber enabled) मुद्दाहरु नै प्रमूख रही कम मात्र साइबर असिस्टेड (Cyber Assisted) रहेको पाईयो । माथिको चार्टबाट ५० मुद्दामा ४९ साइबर इनेबल्ड (cyber enabled) र १ मात्र साइबर असिस्टेड (Cyber Assisted) रहेको देखिन्छ ।

११. कसूरको उद्देश्य



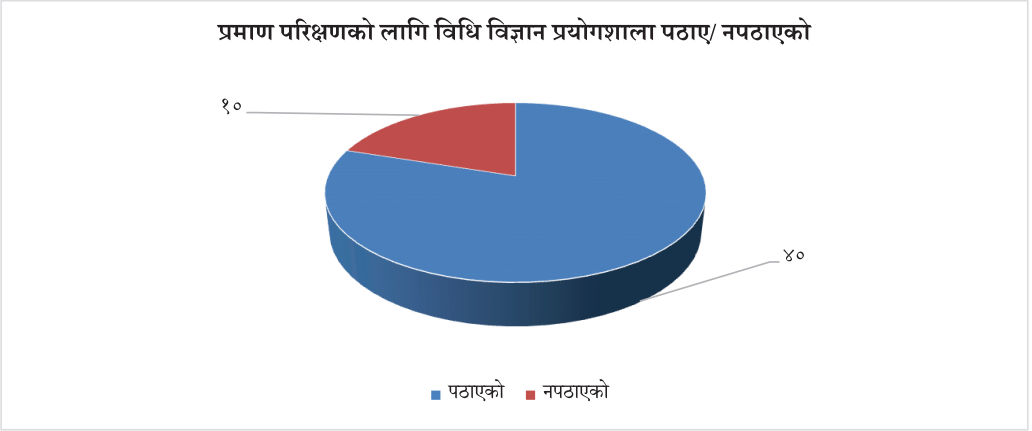
अध्ययन गरिएका मुद्दाहरुबाट साइबर कसूरका कसूरदारहरुहरु मध्य आधा भन्दा बढीको उद्देश्य यौन दुर्व्यवहार रहेको पाईयो। ५० जना कसूरदार मध्ये २६ (५२.००%) जनाको उद्देश्य यौन दुर्व्यवहार, ७ (१४.००%) जनाको उद्देश्य मनोरञ्जन, २(४.००%) जनाको आर्थिक उपार्जन र १५ (३०.००%) जनाको अन्य उद्देश्य रहेको देखियो।

१२. कसूरमा प्रयोग भएको User ID fake भए/नभएको



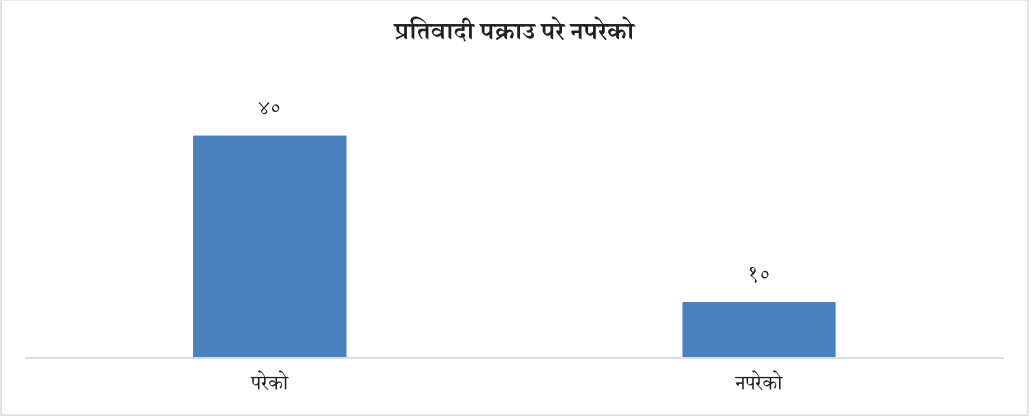
प्रतिवादीहरुले कसूर गर्दा आफ्नो वास्तविक परिचय प्रयोग गर्छन् वा गर्दैनन् भन्ने विषयमा अध्ययन गर्दा ५० मध्ये २६ जनाले झुट्टा परिचयको User ID प्रयोग गरी र २४ ले आफ्नो वास्तविक User ID बाट कसूर गरेको पाईयो।

१३. प्रमाण परिक्षणको लागी विधि विज्ञान प्रयोगशाला पठाए/नपठाएको



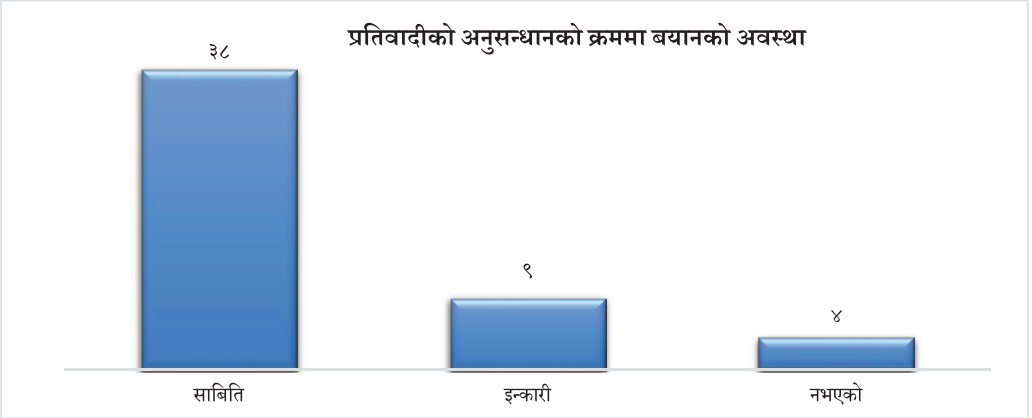
अध्ययन गरिएका ५० मुद्दा मध्ये ४० वटामा प्रमाण परीक्षणको लागी विधि विज्ञान प्रयोगशाला पठाईएको र १० वटामा नपठाइएको पाईयो।

१४. अनुसन्धान तथा अभियोजन गर्दा प्रतिवादी पक्राउ परे/नपरेको



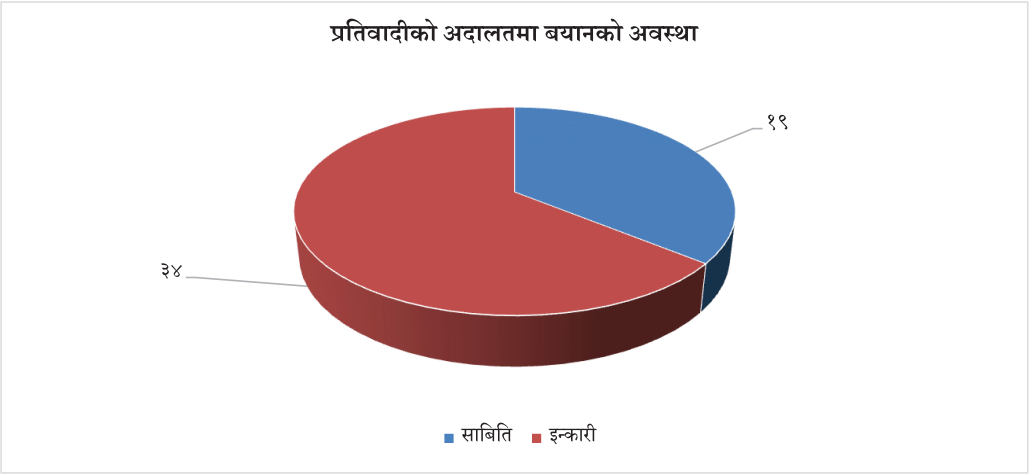
साइबर कसूरमा विशेषगरी थुनामा नै राखेर अनुसन्धान तथा अभियोजन हुने गरेको तथ्य तल प्रस्तुत गरेको चार्टमा उल्लेख भए बमोजिम अध्ययन गरिएका ५० मुद्दा मध्ये ४० वटा मुद्दाका प्रतिवादीहरु अनुसन्धान एवम् अभियोजन गर्दा पक्राउ परेको र बाँकी १० मुद्दामा फरार रहेको तथ्याङ्कबाट देखाउँछ।

१५. प्रतिवादीले अनुसन्धानको क्रममा गरेको वयानको अवस्था



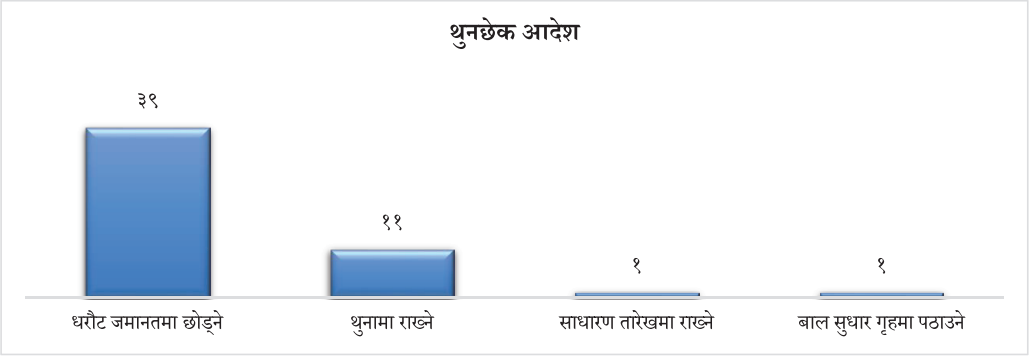
अध्ययन गरिएका मुद्दाहरुमा प्रतिवादीहरुले अनुसन्धानको क्रममा गरेको वयान मध्ये अधिकांशमा प्रतिवादीहरु साविती रहेको पाईयो। ५१ प्रतिवादीहरु मध्ये ३८ जना कसूरमा सावित रहेको, ९ जना इन्कारी रहेको र ४ जनाको हकमा नखुलेको अवस्था थियो।

१६. प्रतिवादीले अदालत समक्ष गरेको वयानको अवस्था



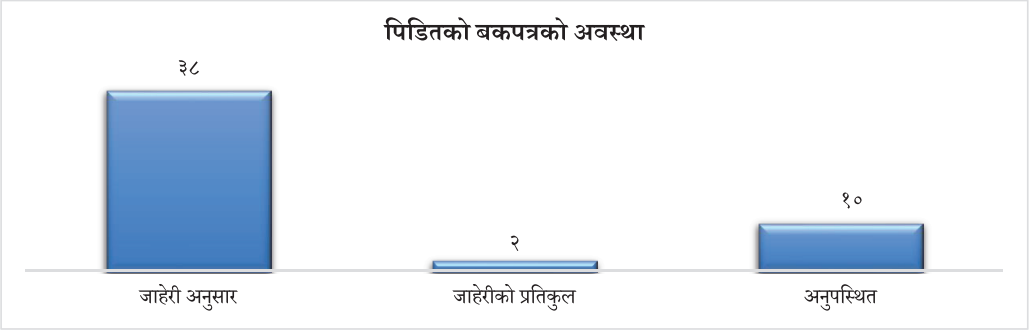
अदालत समक्ष वयान गर्दा भने कसूरमा इन्कार रहने प्रतिवादीको सङ्ख्यख्या बढी रहेको देखियो। अध्ययन गरिएका ५३ प्रतिवादीहरु मध्ये अदालत समक्ष वयान गर्दा १९ जना कसूरमा सावित रहि ३४ जना इन्कार रहेको पाईयो।

१७. थुनछेक आदेश सम्बन्धमा



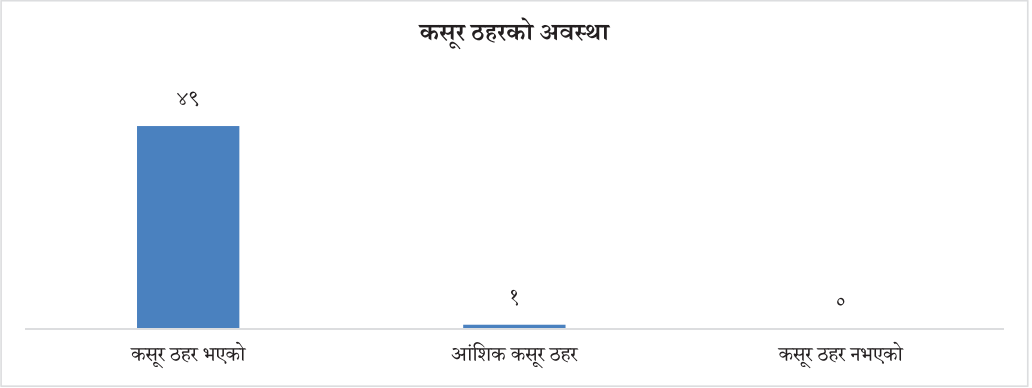
साइबर कसूरका अधिकांश प्रतिवादीहरुलाई थुन्छेकको क्रममा धरौट वा जमानत माग गरी पुर्पक्ष हुने गरेको पाईयो भने केहीलाई थुनामा र अति न्यूनलाई साधारण तारेखमा राख्ने गरेको पाईयो । नाबालक उपर मुद्दा चलेकोमा सुधार गृहमा पठाउने आदेश भएको समेत देखियो । तलको चार्टमा देखिए बमोजिम ५२ जना प्रतिवादीहरुमा ३९ जनालाई धरौट जमानतमा छोड्ने, ११ जनालाई थुनामा राख्ने, १ जनालाई साधारण तारेखमा र एक जनालाई बाल सुधार गृहमा पठाउने गरी आदेश भएको पाईयो ।

१८. पीडितको बकपत्रको अवस्था



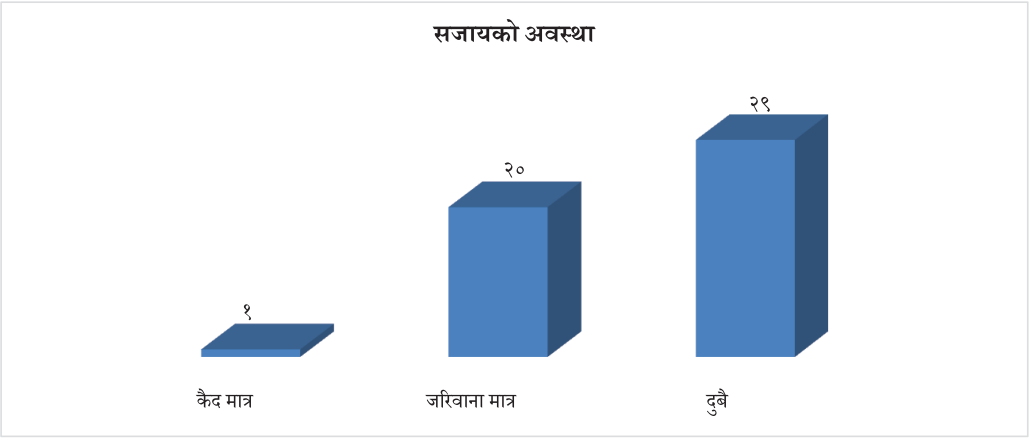
साइबर कसूरका पीडितहरुले जाहेरी अनुरुपकै बकपत्र गर्नेको सङ्ख्या उल्लेख्य देखिई प्रतिकूल बकपत्र निकै कम मुद्दामा हुने गरेको पाईयो । अध्ययन गरिएका ५० जना पीडितहरु मध्ये ३८ जनाले जाहेरी अनुरुपको र २ जनाले मात्र प्रतिकूल बकपत्र गरेको देखियो । १० जना पीडितहरु भने बकपत्रको लागी उपस्थीत नभएको पाईयो ।

१९. कसूर ठहरको अवस्था



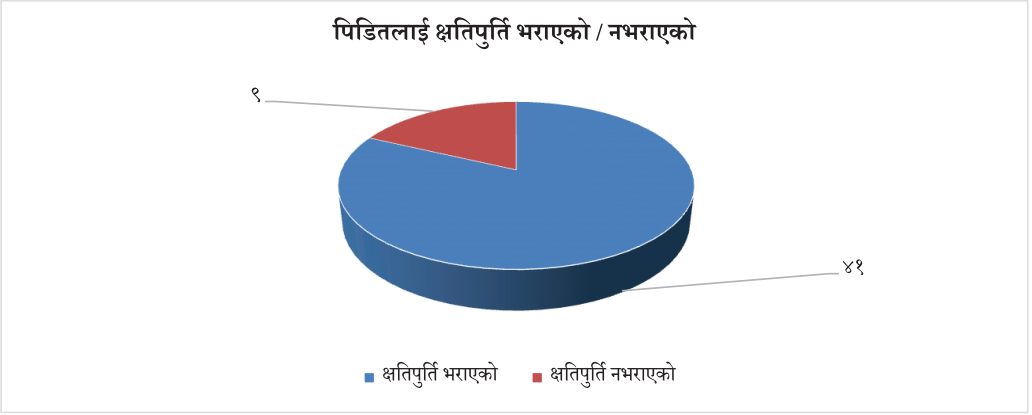
अनुसन्धानबाट साइबर कसूरमा झण्डै सतप्रतिशत सफलता रहेको पाईयो। अनुसन्धान गरिएका ५० थान मुद्दामा ४९ मा कसूर ठहर भएको र १ वटा मुद्दामा आंशिक कसूर ठहर भई सफाई पाउने मुद्दाको सङ्ख्या शून्य देखियो।

२०. सजायको अवस्था



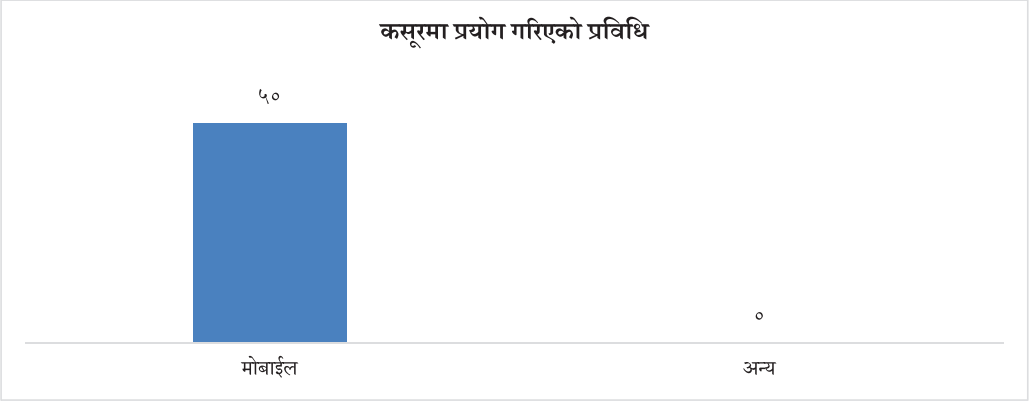
अध्ययन गरिएका मुद्दाको फैसलाको प्रकृति हेर्दा कैद मात्र हुनेगरि, जरिवाना मात्र हुनेगरी र कैद एवम् जरिवाना दुवै हुनेगरी सजाय भएको पाईयो। ५० वटा मध्ये २० वटामा जरिवाना मात्र हुनेगरी, २९ वटामा कैद र जरिवाना दुवै हुनेगरी र १ वटा मुद्दामा कैद मात्र ठहर भएको माथि प्रस्तुत चार्टबाट देख्न सकिन्छ।

२१. पीडितलाई क्षतिपूर्ति भराए/नभराएको



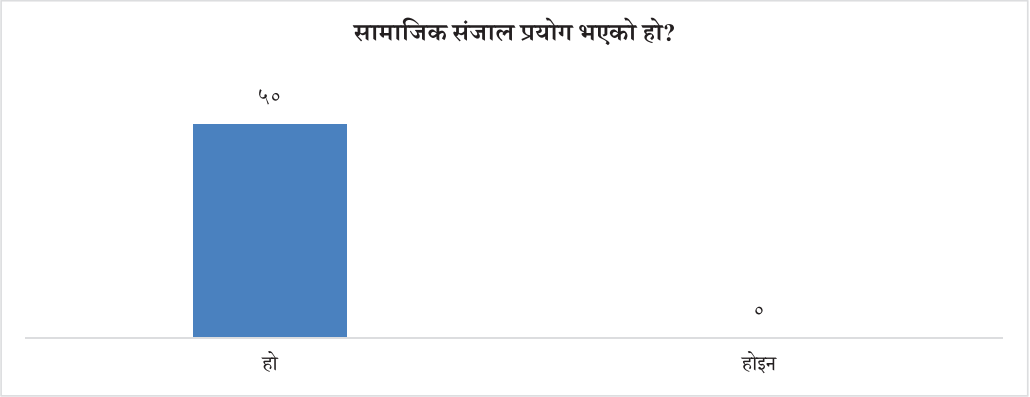
अनुसन्धानबाट साइबर कसूरमा पीडितको क्षतिपूर्ति सम्बन्धि हकको सतप्रतिशत सुनिश्चितता भएको पाईएन । ५० वटा मुद्दामा ४१ वटामा पीडितलाई क्षतिपूर्ति भराउने ठहर भएको पाईयो भने ९ वटामा क्षतिपूर्ति नभराउने गरि फैसला भएको देखियो ।

२२. कसूरमा प्रयोग गरिएको प्रविधि



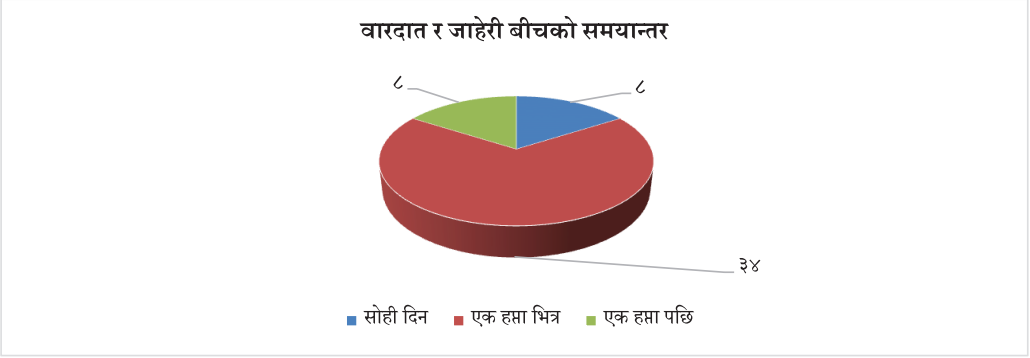
अनुसन्धान गरिएका सबै मुद्दामा प्रतिवादीले मोबाईल फोनको प्रयोगबाट कसूर गरेको पाईयो ।

२३. सामाजिक सञ्जाल प्रयोग भए/नभएको



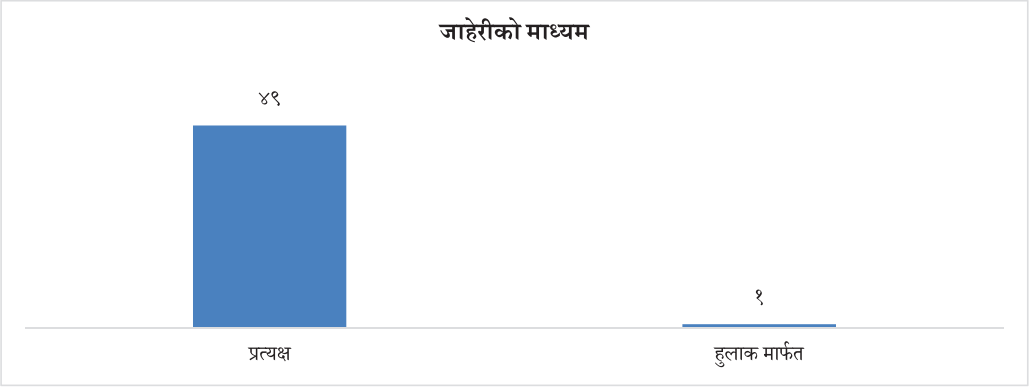
अनुसन्धान गरिएका सबै मुद्दामा सामाजिक संजालको प्रयोग गरेर नै कसूर गरेको पाईयो।

२४. वारदात र जाहेरीबिचको समयान्तर



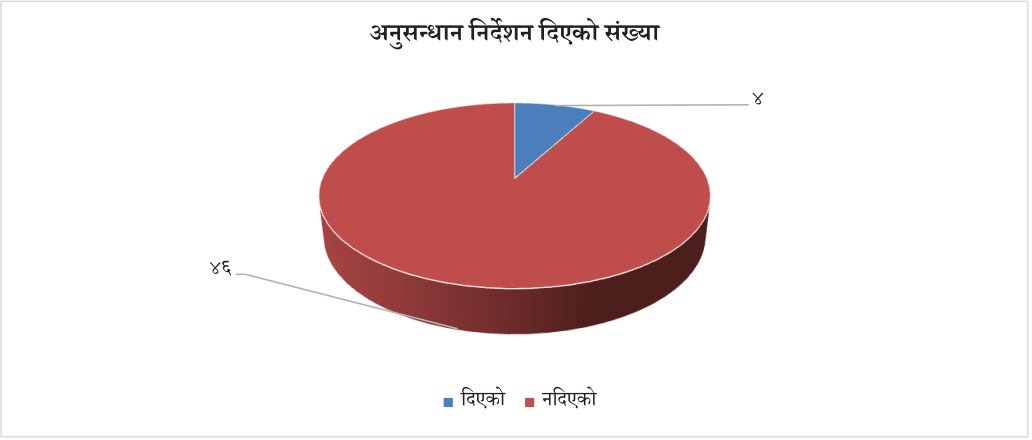
साइबर कसूरमा वारदात र जाहेरीबिचको समायन्तर अध्ययन गर्दा ५० मुद्दा मध्ये ८ वटा मुद्दामा वारदात भएकै दिनमा जाहेरी दर्ता भएको पाईयो भने ३४ वटा मुद्दामा वारदात भएको एक हप्ता भित्र दर्ता भएको पाईयो। ८ वटा मुद्दामा एक हप्ता पछि जाहेरी दर्ता भएको देखियो।

२५. जाहेरीको माध्यम



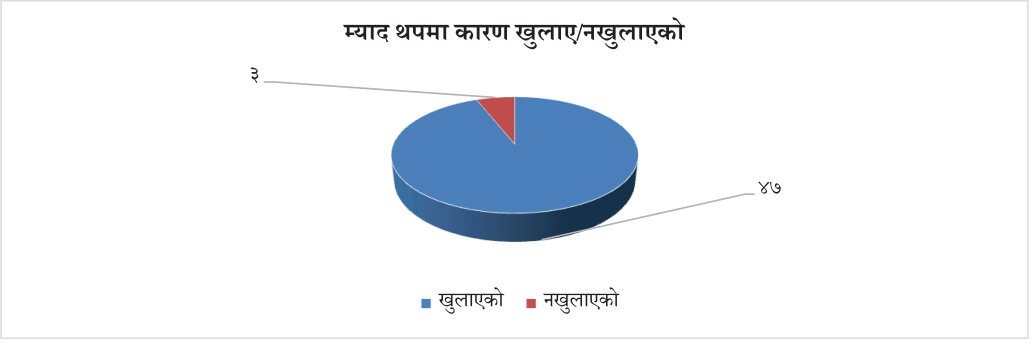
जाहेरी दर्ताको माध्यम हेर्दा अधिकांश मुद्दामा प्रत्यक्ष जाहेरी दर्ता भएको पाईयो भने हुलाक मार्फत समेत दर्ता हुने गरेको देखियो। ५० मुद्दामा ४९ वटा जाहेरी प्रत्यक्ष दर्ता भएको र १ वटा हुलाक मार्फत दर्ता भएको पाईयो।

२६. अनुसन्धान निर्देशन दिएको सङ्ख्या



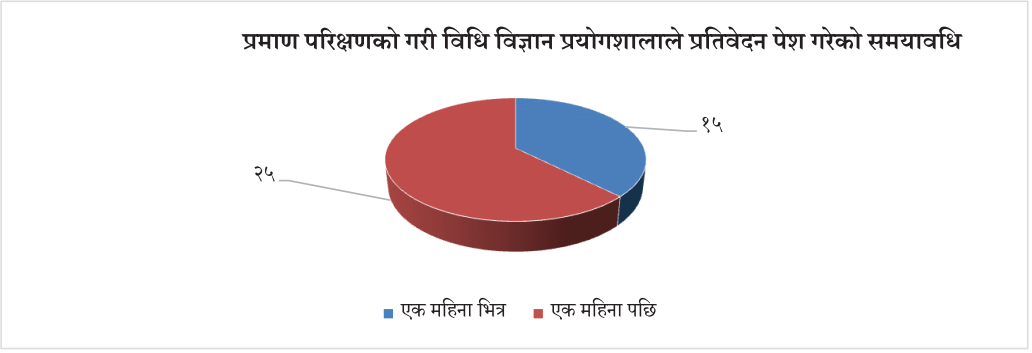
अध्ययन गरिएका ५० मुद्दा मध्ये ४ वटा मुद्दामा मात्र सम्बन्धित सरकारी वकीलबाट अनुसन्धानको क्रममा निर्देशन दिईएको पाईयो।

२७. म्याद थपमा कारण खुलाए/नखुलाएको अवस्था



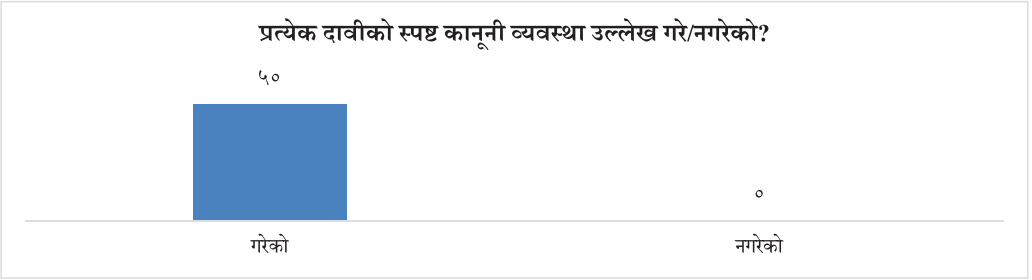
अध्ययन गरिएका मुद्दाहरु मध्ये ४७ वटा मुद्दामा आधार कारण खुलाई म्याद थप गरेको पाईयो भने ३ वटामा नखुलाईएको तथ्याङ्क निम्न बमोजिम प्रस्तुत गरिएको छ।

२८. प्रमाण परिक्षण गरी विधि विज्ञान प्रयोगशालाले प्रतिवेदन पेश गरेको समयावधि



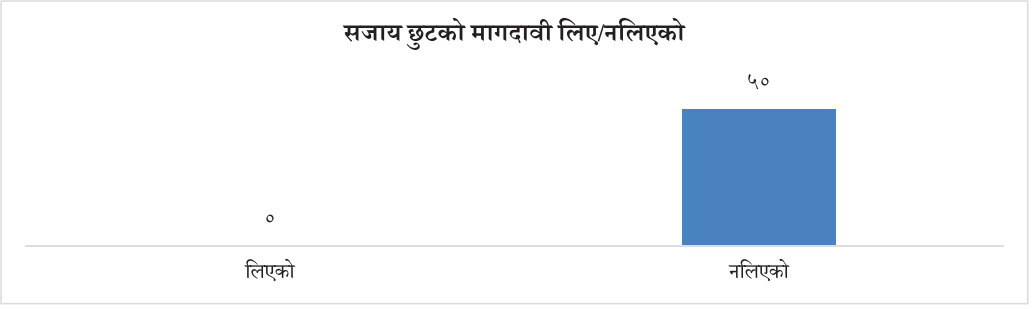
साइबर कसूरमा डिजिटल प्रमाण परिक्षणको लागी विधिविज्ञान प्रयोगशाला पठाईनेमा प्रतिवेदन प्राप्त हुन लाग्ने समयको अध्ययन गर्दा ५० मध्ये १५ वटा मुद्दामा एक महिना भित्र प्रतिवेदन प्राप्त भएको देखियो भने २५ वटामा एक महिनापछि प्राप्त भएको देखियो। चार्ट यस प्रकार रहेको छः

२९. प्रत्येक दावीको स्पष्ट कानुनी व्यवस्था उल्लेख भए/नभएको



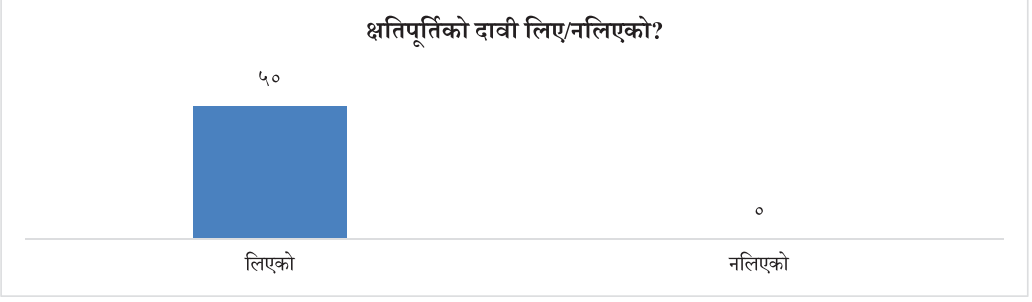
अध्ययन गरिएका सबै मुद्दामा अभियोगपत्रमा अभियोगदावी लिईएको कसूरको स्पष्ट कानुनी व्यवस्था उल्लेख गरेको पाईयो।

३०. सजाय छुटको मागदावी लिए/नलिएको



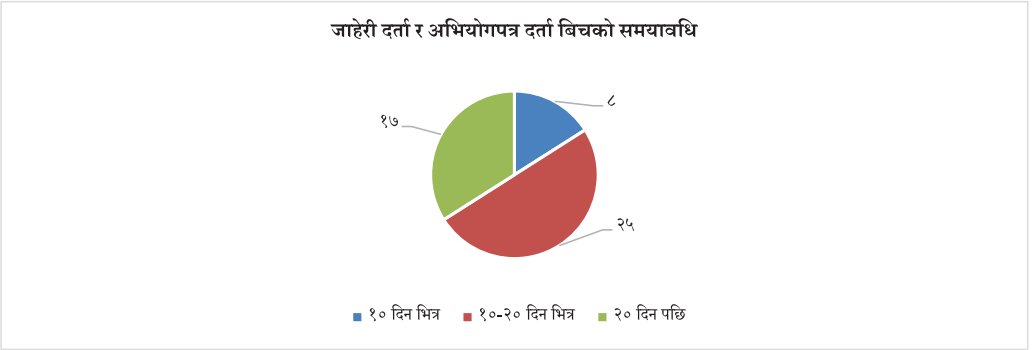
अध्ययनबाट साइबर कसूरमा सजाय छुटको मागदावी लिने प्रचलन शून्य रहेको पाईयो।

३१. क्षतिपूर्तिको दावी लिए/नलिएको



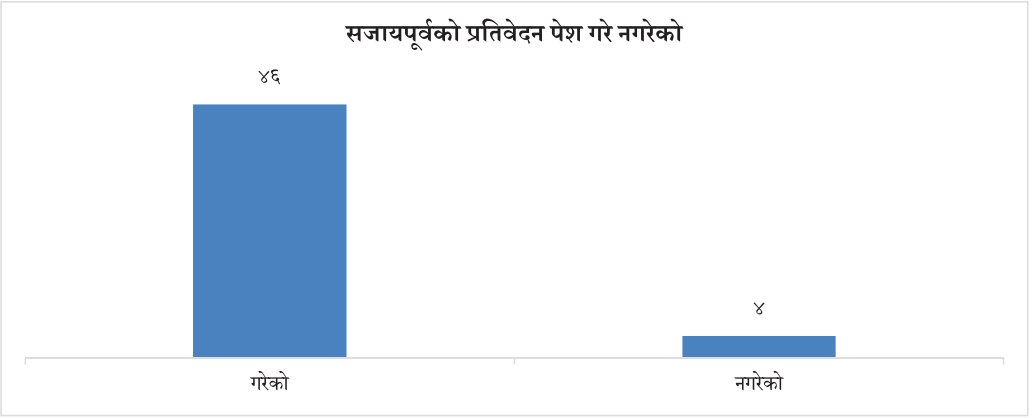
अध्ययन गरिएका ५० वटा मुद्दा सबैमा अभियोगपत्रमा क्षतिपूर्तिको दावी लिएको पाईयो।

३२. जाहेरी दर्ता र अभियोगपत्र दर्ता बिचको समयावधि



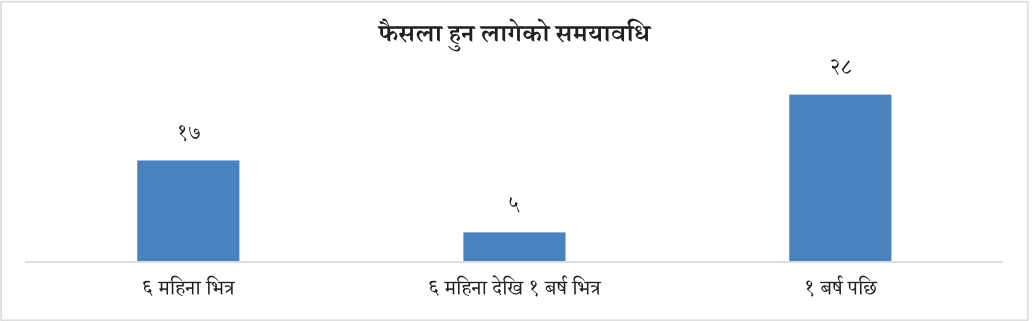
साइबर कसूरमा जाहेरी दर्ता र अभियोगपत्र दर्ता बिचको समयावधी अध्ययन गर्दा ८ वटा मुद्दामा जाहेरी दर्ता भएपछिको १० दिनमा अभियोगपत्र दर्ता भएको देखियो। अधिकांश मुद्दा (२५ वटा) जाहेरी दर्ता गरेको १०-२० दिन भित्र दर्ता भएको र १७ वटा मुद्दामा जाहेरी दर्ता भएको २० दिन पछि दर्ता भएको पाईयो। उक्त तथ्याङ्क तलको चार्टमा प्रस्तुत छः

३३. सजायपूर्वको प्रतिवेदन पेश गरे/नगरेको



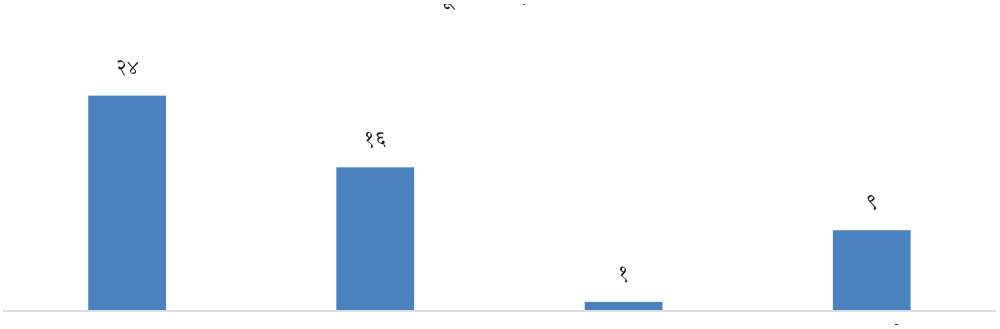
अध्ययन गरिएका ५० मुद्दा मध्ये ४६ वटा मुद्दामा सजायपूर्वको प्रतिवेदन पेश गरेको र ४ वटा मुद्दामा पेश नगरेको माथि प्रस्तुत चार्टबाट देख्न सकिन्छ।

३४. फैसला हुन लागेको समयावधि



साइबर कसूर सम्बन्धि मुद्दामा अभियोगपत्र दर्ता भएपछि फैसला हुन लागेको अवधि अध्ययन गर्दा १७ वटा मुद्दामा तुलनात्मक हिसाबले छिटो मुद्दा फछर्यौट भएको (६ महिना भित्र) पाईयो। माथि प्रस्तुत चार्टमा उल्लेख भए बमोजिम ५ वटा मुद्दामा ६ महिना देखि १ वर्ष भित्र फैसला भएको र बाँकी २८ वटामा १ वर्ष पछि फैसला भएको देखियो।

३५. क्षतिपूर्ति भराएको रकम



फैसलाहरुको अध्ययन गर्दा २५ वटा मुद्दामा रु.२५००० सम्म क्षतिपूर्ति भराउने गरी, १६ वटा मुद्दामा रु.२५,००० देखि रु.५०,००० सम्मको क्षतिपूर्ति भराउने गरी, १ वटा मुद्दामा रु.५०,०००। – भन्दा माथिको रकम क्षतिपूर्ति स्वरुप भराउने गरी फैसला भएको पाईयो। ९ वटा मुद्दामा भने क्षतिपूर्ति भराउने फैसला भएको पाईएन।

६.४. जिल्ला सरकारी वकील कार्यालयबाट प्राप्त अभियोगपत्र र फैसलाको अध्ययन तथा तथ्यांकको विश्लेषणबाट प्राप्त निष्कर्ष

माथि उल्लिखित आ.व. २०७५/०७६ देखि आ.व. २०७९/०८० सम्म पाँच वर्षको साइबर कसूर मुद्दासंग सम्बन्धित ५० विषय छनोट गरी मिसिलको विविध आयाममा अनुसन्धान गरिएको छ। अनुसन्धानको तथ्यांकवाट प्राप्त निष्कर्षलाई सिलसिलेवार रुपमा नतिजाको आधारमा सम्वोधन गर्नु पर्ने नीतिगत, कानूनी, संरचनागत, व्यवस्थापकीय र कार्यविधिगत पाटोलाई देहायबमोजिम प्रस्तुत गरिएको छ।

१. साइबर कसूर मुद्दा र प्रतिवादी संख्याको आधारमा तथ्यांक अध्ययन गर्दा मुद्दा संख्या र प्रतिवादीको संख्यामा त्यति ठूलो फरक पाउन सकिएन । तथापि विद्युतीय कारोबारसम्बन्धी मुद्धाको संख्यामा कमी छैन भन्ने देखियो । यस आधारमा हेर्दा हामीले विद्युतीय कारोबार सम्बन्धी कसूरलाई समसामपेक्ष कानूनमा संसोधान गरी समयसापेक्ष बनाउनु पर्ने देखिन्छ ।

२. साइबर कसूर मुद्दाहरुको फैसलाको अवस्था विश्लेषण गर्दा फछ्यौट संख्या र बाँकी मुद्दामा त्यति ठूलो अन्तर देखिएन । तथापी आगामी दिनमा मुद्दा फछ्यौट्टलाई अझ बढोन्तरी गर्न जनशक्ति र स्रोत साधनको व्यवस्थापनमा आवश्यक ध्यान दिनु पर्ने देखिन्छ ।

३. साइबर कसूर मुद्दाहरुमा कसूर कायमको अवस्था अध्ययन गर्दा सन्तोषजनक नै पाउन सकिन्छ । तथापी साइबर कसूर मुद्दाको सफलता वृद्धि गर्न ऐनले परिकल्पना गरेको छुटै सूचना प्रविधि न्यायाधिकरण गठन गर्ने प्रकियालाई प्राथमिकता दिनुपर्ने देखिन्छ ।

४. साइबर कसूरमा पीडितको उमेर अध्ययन गर्दा युवा समूह बढी मात्रामा रहेको देखियो । वालबालिकाको उमेर समूह पनि राम्रै देखियो । यस आधारमा युवा समूह बढी मात्रा साइबर कसूरमा लाग्नु भनेको हाम्रो शिक्षा प्रणाली युवामैत्री भएन, बालमैत्री भएन, साइबर कसूर न्यूनीकरण लक्षित भएन तसर्थ शिक्षाप्रणालीमा सुधार र युवा र वालबालिका लक्षित जनचेतना सम्बन्धी कार्यक्रम सञ्चालन गर्न कानूनमा नै स्थानीय निकायलाई जिम्मेवार बनाउनु पर्छ ।

५. प्रतिवादीको उमेर संख्या अध्ययन गर्दा युवा समूहको नै बाहुल्यता रहेको पाइयो । तसर्थ साइबर कसूरको अनुसन्धान तथा अभियोजनमा युवा समूह केन्द्रित हुनुपर्ने देखिन्छ ।

६. पीडितको उमेर संख्या अध्ययन गर्दा महिलाहरु नै विधुतीय कारोवार सम्बन्धी कसूरको जोखिममा परेका देखियो । तसर्थ महिला मैत्री कानून निर्माणमा जोड दिदै अनुसन्धान र अभियोजन पीडित पक्ष केन्द्रित गर्ने र महिला लक्षित जनचेतना सम्बन्धी कार्यक्रम सञ्चालन गर्न कानूनमा नै स्थानीय निकायलाई जिम्मेवार बनाउनु पर्ने देखिन्छ ।

७. प्रतिवादीहरुको लिंग संख्या अध्ययन गर्दा पीडितको उमेर संख्याको ठीक उल्टो पुरुषहरुको संख्या बढी देखियो तसर्थ अनुसन्धान तथा अभियोजन पुरुष समूह लक्षित गर्नुपर्ने देखिन्छ ।

८. विद्युतीय कारोबार सम्बन्धी कसूर विशेष गरी सामाजिक सञ्जालको प्रयोगबाट कसूर भएको संख्या बढी पाइयो । जसमा फेसबुक, टिकटक जस्ता सामाजिक सञ्चालनको नियमन, व्यवस्थापन, समूचित प्रयोग र नियन्त्रण सम्बन्धमा जिम्मेवार निकाय तोक्ने र सामाजिक सञ्जाल प्रयोगमा नियन्त्रणमुखी कानून आवश्यकता देखिन्छ ।

९. पीडित र प्रतिवादी बीचको सम्बन्ध अध्ययन गर्दा बढी चिनजानका व्यक्तिहरु बढी जोखिममा रहेको अवस्था देखियो । साइबर सम्बन्धी कसूरमा अनुसन्धान तथा अभियोजन गर्दा नाता र नजिकको छिमेकी लक्षित हुनुपर्ने देखियो । कानून निर्माण गर्दा पनि नजिकको नातामा साइबर कसूर भएमा बढी सजाय हुने गरी कानून प्रस्ताव गर्नु पर्ने देखिन्छ ।

१०. प्रतिवादीको पेशा अध्ययन गर्दा बढी मात्रामा पेशा व्यवसायमा रहेको व्यक्ति नै साइबर कसूरमा संलग्न भएको पाइयो । । तसर्थ अनुसन्धान र अभियोजन गर्दा पेशा व्यवसाय नजिक पुग्नु पर्ने देखिन्छ । पेशा व्यवसाय गरी कसैले साइबर कसूर गरेमा थप सजायको व्यवस्था गर्ने गरी कानून निर्माण गर्नुपर्छ । विद्यार्थी र वेरोजगार समूह पनि साइवर कसूरमा संलग्न भएको संख्या पनि राम्रै देखियो तसर्थ विद्यार्थी लक्षित जनचेतना कार्यक्रम र पाठयपुस्तकमा सुधार

तथा वेरोजगार लक्षित कार्यक्रम र विकास निर्माण गर्न स्थानीय निकायलाई जिम्मेवार बनाउनु पर्ने देखिन्छ ।

११. वारदातको समयमा देश बाहिर भन्दा देश भित्र नै प्रतिवादी रहेको संख्या बढी देखियो । तसर्थ पहिलो प्राथमिकता भनेको देशभित्र नै अनुसन्धान र अभियोजन लक्षित गर्नुपर्ने देखियो । सूचना प्रविधिको विकाससँगै देश वाहिर पनि प्रतिवादीको संख्या राम्रै पाउँन सकिन्छ । साइबर कसूरको क्षेत्राधिकार वहिक्षेत्रीय बनाउनु पर्छ ।

१२. साइबर कसूरको प्रवृति हेर्दा साइबर असिस्टेड भन्दा साइबर इनेल्वड मुद्दाहरु नै बढी देखिन्छ तसर्थ साइबर कसूरमा कम्प्युटर लक्षित कसूर भन्दा कम्प्युटर विना पनि कसूर हुन्छ भन्ने देखिएकोले सो कानून निर्माण गर्दा सो तर्फ पनि ध्यान दिनु पर्ने देखिन्छ ।

१३. साइबर कसूरका कसूरहरुमा बढी मात्रामा यौन दुरव्यवहार रहेको पाइयो । यस आधारमा यौन दुरव्यवहार लक्षित अनुसन्धान, अभियोजन र कानून निर्माण गरी सजायको मात्रा तोक्नु पर्ने देखिन्छ ।

१४. कसूरमा प्रयोग भएको युजर आइडी हेर्दा झुट्टा परिचयको प्रयोग बढी देखियो यस आधारमा फेक युजर आइडी प्रयोग लक्षित अनुसन्धान र अभियोजन केन्द्रित गर्ने र सोही मुताविक कानूनी व्यवस्था गर्नपर्ने देखिन्छ ।

१५. प्रमाण परीक्षणको लागि विधिविज्ञान प्रयोगशालामा पठाइएको भन्दा नपठाएको संख्या कमी नै देखियो । तसर्थ कसूरको प्रकृति र अवस्था अनुसार विधि विज्ञानको प्रयोगलाई अनिवार्य प्रमाण परीक्षण गरी अनुसन्धान, अभियोजन गर्ने गरी कानून निर्माण आवश्यक देखिन्छ ।

१६. अनुसन्धान तथा अभियोजन गर्दा प्रतिवादी पक्राउको संख्या बढी र फरारको संख्या केही कम देखियो । तसर्थ साइबर कसूरमा सजायको मात्रा बढाई पक्राउ गर्ने तर्फ हाम्रा सुरक्षा संयन्त्रलाई चुस्तदुस्त राख्ने पद्दति विकास गर्न आवश्यक देखिन्छ ।

१७. प्रतिवादीहरुले अनुसन्धानको क्रममा गरेको वयान मध्ये सावितीको संख्या बढी र इन्कारीको संख्या कम नै देखियो । तसर्थ कानून निर्माण गर्दा सावितीं हुनेलाई दावी छुट दिने प्रावधानलाई राख्नुपर्ने देखिन्छ । सोही मुताविक अनुसन्धान र अभियोजन गरिनुपर्छ । इन्कारीको हकमा कडा कानून बनाउनु पर्ने देखिन्छ ।

१८. प्रतिवादीले अदालत समक्ष बयान गर्दा सावितीं भन्दा इन्कारीको संख्या बढी देखियो । यस आधारमा अनुसन्धान तथा अभियोजन क्रममा बयानलाई वस्तुनिष्ट बनाउनुपर्छ । अन्य थप प्रमाणद्धारा पुष्टि गर्ने आधार निर्माण गर्नुपर्छ । अदालतमा इन्कारी बयान गर्ने साक्षी लक्षित कानून बनाउनुपर्छ ।

१९. थुनछेक आदेश हेर्दा थुनाभन्दा धरौटीलाई प्राथमिकता राखेको देखियो । आगामी दिनमा अझ बढी साइबर कसूरमा वृद्धि हुने, कसूरको प्रकृति र अवस्था पनि जटिल हुने तथा सामाजिक सञ्चारको प्रयोग गरेर साइबर कसूर हुने अवस्था देखिँदा सजायको मात्रामा वृद्धि गरी थुनामा नै राखी कारवाही गर्ने व्यवस्था गर्नुपर्ने देखिन्छ ।

२०. साइबर कसूर पीडितहरुको जाहेरी अनुरुप कै वकपत्र गर्ने संख्या उल्लेख तथापि प्रतिकूल वकपत्र गर्ने र वकपत्रका लागि अनुपस्थित हुने संख्या पनि अनुसन्धानबाट पाइएकोले कानून निर्माण गर्दा प्रतिकूल वकपत्र गर्नेलाई कडा सजायको प्रावधान राख्ने र अनुपस्थित हुनेका हकमा अनुसन्धान तथा अभियोजन अधिकारीको सक्रियताका साथै साक्षीलाई दिइने भत्तामा पनि वृद्धि गर्नुपर्ने आवश्यकता देखिन्छ ।

२१. अनुसन्धानबाट साइबर कसूर कसूर ठहरको सफलता राम्रै पाइयो, तसर्थ प्राप्त उपलब्धि जगेर्ना गर्दै आगामी दिनमा अनुसन्धानकर्ता र अभियोजनकर्ताको अतिरिक्त न्यायिक अधिकारीको उच्च मनोवल कायम राख्न थप प्रोत्साहन कार्यक्रम लागू गर्नु पर्ने देखिन्छ ।

२२. अध्ययन गरिएका मुद्दाको फैसलाको प्रकृति हेर्दा धेरै मात्रामा कैद र जरीवानाको सजाय गरेको पाइयो । तसर्थ आगामी दिनमा कानून बनाउदा नै कैदको सजाय मात्र गर्ने आधार र प्रकृति, कैद र जरीवानाको सजाय गर्ने कसूरको प्रकृति र आधार तथा जरीवानाको सजाय गर्ने प्रकृति र आधार स्पष्ट तोक्नुपर्ने देखिन्छ ।

२३. साइबर कसूरमा पीडितको क्षतिपूर्ति सम्बन्धी कानूनी व्यवस्था सत प्रतिशत कार्यान्वयन गरेको पाइएन । तसर्थ आगामी दिनमा कानून निर्माण गर्दा क्षतिपूर्ति विधिशास्त्रको पूर्ण कार्यान्वयन गर्ने गरी कानून निर्माण गर्नुपर्ने देखिन्छ ।

२४. अनुसन्धान गरिएका सबै मुद्दामा प्रतिवादीले मोवाइल फोनको प्रयोगलाई आधार लिएको हुँदा मोबाइल फोन प्रयोगकर्ताको गोपनीयताको हकको सम्मान गर्दै सुक्ष्म अनुगमन र निगरानी अधिकारीको व्यवस्था कानूनमा नै गरी टेलिकमलाई जिम्मेवारी बनाउने, मोबाइल धनीलाई पनि जिम्मेवार बनाउने, मोबाइल फोनको ट्र्याकिङ्गलाई अनुसन्धान र अभियोजनमा पहिलो प्राथमिकता दिने र न्यायिक अधिकारीले समेत फोन ट्र्याकिङ्गबाट प्राप्त प्रमाणलाई मान्यता दिने गरी कानून निर्माण गर्नुपर्ने देखियो ।

२५. अनुसन्धान गरिएका सबै मुद्दामा सामाजिक सञ्जालको प्रयोग गरेको पाइएकाले सामाजिक सञ्चालको प्रकृति छुटाउने, सामाजिक सञ्जालको नियमन अधिकारी तोक्ने, सामाजिक सञ्जाल प्रयोगकर्तालाई जिम्मेवार बनाउने, फेक आइडी बनाउनेलाई कडा भन्दा कडा कारबाही गर्ने गरी कानून निर्माण गर्नुपर्ने देखियो ।

२६. जाहेरी दर्ताको माध्यम हेर्दा प्रत्यक्ष जाहेरी दर्तालाई पहिलो प्राथमिकतामा राखेको पाइयो । आगामी दिनमा यसलाई निरन्तरता दिनुपर्ने देखियो । साथै सूचना प्रविधिको माग दिनदिनै बढी रहेको अवस्थामा हाम्रो अनुसन्धान, अभियोजन र न्याय सम्पादन पनि सूचना मैत्री बनाउन आवश्यक देखिन्छ । यसका लागि तिनै निकाय बीच Joint E System बिकास गर्न जनशक्ति, बजेट र कानूनको आवश्यकता देखियो ।

२७. अनुसन्धानमा अभियोजन अधिकारीले दिएको निर्देशन संख्या हेर्दा निर्देशन संख्या न्यून पाइयो । आगामी दिनमा सम्बन्धित सरकारी वकीललाई प्रत्येक मुद्दामा अनिवार्य लिखित निर्देशन दिने गरी कानून निर्माण गर्नुपर्ने र यसलाई वृत्ति विकासका जोडी प्रोत्साहित गर्ने गरी कानून संसोधन गर्नुपर्छ ।

२८. म्याद थपमा आधार र कानून खुलाई म्याद थप गरेको संख्या बढी भएतापनि म्याद थपमा आधार र कानून नखुलाएको पनि पाइयो । त्यसैले आगामी दिनमा साइवर कसूरमा म्याद थप माग गर्दा अनिवार्य रुपमा आधार र कारण खुलाउने गरी कानून निर्माण गर्नुपर्ने देखियो ।

२९. प्रमाण परीक्षण गरी विधि विज्ञान प्रयोगशालाले एक महिनाको समयमा प्रतिवेदन पेश भएको संख्या बढी पाइयो । आगामी दिनमा विधि विज्ञान प्रयोगशालाको संख्या वृद्धी गर्ने,साइबर कसूरको परीक्षण गर्ने र प्रतिवेदन दिने छुटै शाखा रहने गरी कानून बनाउन पर्ने देखिन्छ । विधि विज्ञान प्रयोगशाला अनिवार्य रुपमा सबै प्रदेशमा स्थापना गर्न सरकारलाई जिम्मेवार बनाउनुपर्ने देखिन्छ ।

३०. अध्ययन गरिएका सबै मुद्दामा अभियोगपत्रमा अभियोगदावी लिएको कसूरमा स्पष्ट कानून व्यवस्था गरेको पाईयो । यसलाई आगामी दिनमा पनि निरन्तरता दिने साथै साइबर कसूरमा मुद्दाको प्रकृति, कानून, क्षतिपूर्ति र दिगो दावी सम्बन्धी स्पस्ट कानून बन्नु पर्ने देखिन्छ ।

३१. अध्ययनबाट साइबर कसूरमा सजाय छुटको मागदावी लिने प्रचलन शुन्य पाइयो । आगामी दिनमा सजायमा दावी छुटलाई पहिलो प्राथमिकतामा राख्ने गरी कानून बनाउने, दावी छुट बढी लिने अनुसन्धान कर्ता, अभियोजनकर्ता र न्यायिक अधिकारीको नाम वार्षिक प्रतिवेदनमा समावेश गर्ने साथै पुरस्कृत गर्ने व्यवस्था समेत गर्नुपर्ने देखियो ।

दावी छुट लिने जनशक्तिका लागि तालिम, विदेश भ्रमण र वृत्ति विकासमा समेत जोडनुपर्ने देखियो । सजायमा दावी छुट लिने निर्देशिका, २०८० कार्यान्वयन गर्न थप तालिम सञ्चालन गर्नुपर्ने देखिन्छ ।

३२. अध्ययन गरिएका सबै मुद्दामा क्षतिपूर्ति दावी लिएको पाइयो । यो सकारात्मक कदम भएको देखिन्छ । कानूनमा पनि बालक, वृद्ध, अपाङ्ग भएका पीडितको हकमा बढी क्षतिपूर्ति दिने गरी कानून निर्माण गर्नुपर्ने देखिन्छ ।

३३. जाहेरी दर्ता र अभियोग दर्ता बीचको समयावधि अध्ययन गर्दा अधिकांश मुद्दामा २० दिन भित्र अभियोग दर्ता गरेको पाइयो । अभियोग दर्तालाई वस्तुनिष्ट र वैज्ञानिक प्रमाणमा आधारित बनाउने गरी कानून निर्माण गर्नुपर्ने देखिन्छ ।

३४. सजायपूर्वको प्रतिवेदन पेश गरेको संख्या बढी भएतापनि पेश नगर्ने संख्या पनि पाइयो तसर्थ सजाय पूर्वको प्रतिवेदनलाई अनिवार्य गर्ने साथै साइबर कसूरमा सजाय पूर्वको प्रतिवेदन पेश गर्ने अधिकारी कानूनमा नै तोक्नु पर्ने देखिन्छ ।

३५. साइबर कसूरमा एक वर्ष पछि फैसला हुने संख्या बढी पाइयो । साइवर कसूरमा संक्षिप्त कार्यविधि हुने भनी कानून निर्माण गर्नुपर्ने देखिन्छ ।

३६. क्षतिपूर्ति भराएको संख्या हेर्दा सामान्य क्षतिपूर्ति मात्र भराएको पाइयो । आगामी दिनमा कानून निर्माण गर्दा मुद्दाको प्रकृति र अवस्था हेरी क्षतिपूर्ति रकम निर्धारण गर्ने गरी कानून बनाउन पर्ने देखिन्छ ।

परिच्छेद सात

अध्ययनमा देखिएका समस्या र चुनौतीहरू, सुझाव तथा निष्कर्ष

७.१. साइबर कसूरको अनुसन्धान र अभियोजनमा रहेको समस्या र चुनौतीहरू (Problems and Challenges of Investigation and Prosecution on Cyber Crime)

विद्युतीय कारोबार ऐन विद्युतीय तथ्यांक आदानप्रदानको माध्यमबाट वा विद्युतीय सञ्चार माध्यमबाट हुने कारोबारलाई नियमित र व्यवस्थित गर्न आएको देखिन्छ। यसमा अभिलेख तथा डिजिटल हस्ताक्षरसम्बन्धी व्यवस्था अन्तर्गत यसले विद्युतीय अभिलेखको प्रमाणिकता, विद्युतीय अभिलेख र डिजिटल हस्ताक्षरको कानुनी मान्यता, सुरक्षित विद्युतीय अभिलेख, सुरक्षित डिजिटल हस्ताक्षरसम्बन्धी व्यवस्थाहरू रहेका छन्। त्यसैगरी विद्युतीय अभिलेखको सम्प्रेषण, प्राप्ति र स्वीकार, नियन्त्रण तथा प्रमाणीकरण गर्ने निकायसम्बन्धी व्यवस्था, डिजिटल हस्ताक्षर तथा प्रमाणसम्बन्धी व्यवस्था, ग्राहकको काम कर्तव्य र अधिकार, विद्युतीय अभिलेख र डिजिटल हस्ताक्षरको सरकारी प्रयोग, नेटवर्क सेवासम्बन्धी व्यवस्थाहरू रहेको र यी व्यवस्थाहरू उल्लंघन गर्ने वा निषेधित कार्य उपर कम्प्युटरसम्बन्धी कसूर अन्तर्गत सजायको व्यवस्था गरिएको छ। जसमा कम्प्युटर स्रोत संकेतको चोरी, नष्ट वा परिवर्तन गर्न, कम्प्युटर सामग्रीमा अनधिकृत पहुँच, कम्प्युटर सूचना प्रणालीमा क्षति, विद्युतीय स्वरूपमा गैरकानुनी कुरा प्रकाशन, गोपनीयता भंग, झुट्ठा बेहोराको सूचना, झुट्ठा इजाजतपत्र वा प्रमाणपत्र पेस गर्ने वा देखाउने, तोकिएको विवरण वा कागजात दाखिला नगर्ने, कम्प्युटर जालसाजी, कम्प्युटरसम्बन्धी कसूर गर्न दुरुत्साहन, मतियार लगायतका कार्यउपर सजाय रहेको छ।

इन्टरनेटको प्रयोगमार्फत गरिने चरित्र हत्या, हिंसा फैलाउने कार्य, यौनजन्य हिंसा, इण्टरनेट फ्रड, अर्काको पहिचान अनाधिकृत रूपमा प्रयोग, क्रेडिट कार्ड तथा एकाउण्ट आदिको चोरी गरी गरिने बैङ्किङ कसुर, अर्काको कम्प्युटर, विद्युतीय उपकरण तथा नेटवर्कमा पुर्याउने क्षति लगायत अवैधानिक कार्यहरु दिनानुदिन बढिरहेका छन्। अब फायरवेल र एन्टिभाइरसले मात्रै साइबर थ्रेट नरोकिने भएकाले उच्च तहको सेक्युरिटी थ्रेटलाई सम्बोधन गर्नुपर्ने चुनौती छ। अहिले एटीएम, अनलाइन बैंकिङ्ग, मोबाइल बैंकिङ्ग, एसमएस बैंकिङका सुविधासँगै गम्भीर चुनौति पनि बढ्न थालेका छन्। यो परिस्थतिमा ऐनको कार्यान्वयमा देखिएका समस्या तथा चुनौतीहरु यस प्रकार रहेको छ।

१. विद्युतीय (इलेक्ट्रोनिक) कारोबार तथा सूचना प्रविधिको विकासले दिनानुदिन फड्को मारिरहेको अबस्थामा यो ऐन सापेक्षरुपमा परिमार्जन हुन नसक्दा अपेक्षा गरिए अनुरुप विद्युतीय (इलेक्ट्रोनिक) कारोबारको नियमन र साइबर कसूरको नियन्त्रण हुन नसकेको।

२. यो ऐन कसूरको नियन्त्रण गर्न नभई विद्युतीय सञ्चार माध्यमबाट हुने कारोबारलाई प्रमाणीकरण र नियमित गर्न ल्याइएको देखिएकोले कसूरको नियन्त्रण र सजायको अबस्था कमजोर देखिएको।

३. नेपालमा सबैभन्दा बढी सामाजिक सञ्जालबाट साइबर कसूर हुने गरेको छ। यस्ता कसूरहरु परिभाषित हुन नसक्दा अनुसन्धान तथा अभियोजनमा कानुनी जटिलता रहेको।

४. इमेल हैरानी, साइबर स्ट्याल्किङ, अश्लील सामग्री फैलाउनु, इन्टरनेग मार्फत गरिने गालीबेइज्जती, ह्याकिङ, क्रयाकिङ, इमेल ठगी, एसएमएस ठगी, कार्डिङ ठगी एवं धोखेबाजी, बाल पोर्नोग्राफी, इमेल वा एसएमएस

धम्कीद्वारा कुटपीट, साइबर स्क्वाटिङ, साइबर भेन्डालिज्म, कम्प्युटर सिस्टम ह्याकिङ, भाइरस पठाउने, साइबर ट्रेसपास, इन्टरनेटमार्फत चोरी, साइबर टेरोरिज्म, साइबर वारफेयर, पाइरेटेड सफ्टवेयर वितरण, अनधिकृत सूचनाको भण्डारणहरू, बाल पोर्नोग्राफी, साइबर ट्राफिकिङ, आर्थिक कसूर र कीर्ते, स्पाम इमेल र फिसिङ, अनलाइन स्क्याम र जालसाजी, अनलाइन कारोबारमा हुने ठगी, आइडेन्टिटी थेफ्ट, साइबर बुलिइङ, कम्प्युटर प्रणालीमा आक्रमण एवं गैरकानुनी वा निषेधित अनलाइन सेवा संचालन, अफसेन्स, अनलाइन एलोरिङ आदी जस्ता विषयहरुलाई स्पष्ट गरी कसुर कायम नगरिँदा अपराधीहरुले सजाय नपाउने अबस्था रहेको छ।

५. विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ ले सबै किसिमका साइबर कसूरलाई समेट्न नसकेको र यसको परिभाषाभन्दा बाहिरका कसूरमा पनि यही ऐन आकर्षित गरिंदा अपराधिहरु उम्किने खतरा रहेको।

६. यसमा पीडितलाई क्षतिपूर्ति र पीडकलाई उचित दण्ड र जरिवानाबारे समय सापेक्ष व्यवस्था नरहेकोले पीडक फेरि पनि कसूर गर्न हौसिने अवस्था रहेको।

७. ऐनमा गोपनीयताको हकलाई यथोचित स्थान नदिएकोले पीडितको गोपनीयता कायम हुन नसकेको साथै गोपनीयता भङ्ग हुने डरले पीडितहरु पीडा लुकायर बस्ने गरेको।

८. यस ऐनमा बहु क्षेत्राधिकार आकर्षित रहेको भएता पनि विदेशी राष्ट्र समक्ष पारस्परिक कानुनी सहायता सम्बन्धि सम्झौता तथा सुपुर्दगी सन्धि नहुँदा कसूरको अनुसन्धानमा जटिलता रहेको।

९. विद्युतीय कसूरहरु गम्भिर प्रकृतिको हुने गरेको, यसको अनुसन्धान तथा विद्युतीय उपकरणको परीक्षणमा समय लाग्ने भएकोले ३५ दिनको हदम्याद कम रहेको।

१०. साक्षी संरक्षणको विषयलाई कानुनमा उल्लेख नहुँदा साक्षीहरुबाट मुद्दामा उल्लेख्य सहयोग हुन नसकेको।

११. विद्युतीय कसूरको अनुसन्धान तथा अभियोजन गर्ने जनशक्तिमा ज्ञान, सीप, क्षमताको कमी

१२. विद्युतीय कसूरमा प्रयोग भएको प्रविधिको परीक्षण गर्ने दक्ष जनशक्ति र प्रविधीको कमी

१३. विद्युतीय कसूरमा अनुसन्धान गर्ने कर्मचारी तथा प्रविधिको परीक्षण गर्ने जनशक्तिमा कमजोर उत्प्रेरणा र मनोबल।

१४. विद्युतीय कसूरको अनुसन्धान गर्ने कार्य राज्यको प्राथमिकतामा नपर्नु

१५. नीजी तथा सरकारी क्षेत्रहरु डिजिटल सुरक्षा प्रणाली दह्रो बनाउने, आफ्ना सामग्री बढीभन्दा बढी सुरक्षित राख्नेतर्फ सचेत नहुने गरेको

१६. नेपालका नीति निर्माता, प्रविधिविज्ञ, सुरक्षाविज्ञको प्राथमिकतामा साइबर सुरक्षा नपरेको

१७. कसूर अनुसन्धान र तहकीकातको लागि सूचना प्रविधि सम्बन्धी विशेष दखल भएका साइबर प्रहरी र प्रमाणको परीक्षण गर्ने गुणस्तरीय साइबर फोरेन्सीक ल्यावको अभाव।

१८. साइबर कसूरविरुद्धको अभियानमा राज्यको लगानी कमजोर हुने गरेको

१९. प्रमाण संकलनदेखि अदालती कारबाहीसम्मको चेन अफ कस्टडी मेनटेन गर्ने कानुनी व्यवस्था नरहेको।

२०. विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ सँग कसूर संहिता, प्रतिलिपी अधिकारका केही प्राबधानहरु बाझिएकोले कार्यान्वयनमा विरोधाभाष देखिएको।

नेपालले हालसम्म कुनै पनि देशसँग Mutual Legal Assistance Treaty (MLAT) नगरेको हुँदा विद्युतीय सूचनाको उत्पत्तिकर्ता राष्ट्रसंग नेपालले नियन्त्रणकारी अनुगमनका लागि सुचनाको पहुंच पुर्याउन नसक्दा फेसबुक,

जीमेल, याहु जस्ता निकायको सहयोग प्राप्त हुन नसकेको। सूचना प्रविधिको द्रुत विकास र बढ्दो प्रयोगसंगै आपराधिक क्रियाकलापमा समेत यसको दुरूपयोगका कारण कसूरका नयाँ-नयाँ शैली र प्रवृतिले कसूर अनुसन्धान तथा अभियोजन सम्बन्धी कार्य थप चुनौतीपूर्ण भएको छ। साइबर कसूरको अनुसन्धान र अभियोजनमा रहेको समस्या र चुनौतीहरूलाई यस प्रकार उल्लेख गरिएको छ।

१. **कसूरको स्वरूपमा परिवर्तन**: नेपालमा २०६३ सालमा बनेको विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐनको आधारमा अनुसन्धान र अभियोजनको कार्य हुदै आएको छ। यस ऐनले सबै किसिमका साइबर कसूर यसले समेट्न नसकेको भनी आलोचना हुँदै आएको छ। यस ऐनमा अपराधिकरण गरिएको बाहेकका कसुरमा समेत यही ऐनको प्रावधान आकर्षित गरिंदा थप आलोचना हुने गरेको छ। विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐनको निर्माण हुँदाको समयमा फेसबुक, ट्वीटर, भाइबरजस्ता थुप्रै सामाजिक सञ्जालहरूको प्रयोग अहिलेको जस्तो ब्यापक भइनसकेको कारण ति विषयलाई ऐनले समेट्न सकेको अवस्था छैन। अहिले साइबर कसूरको स्वरूप, शैली, मोडस अपरेण्डी (Modus Operandi) मा व्यापक परिवर्तन भएको छ। १५ वर्ष अघिको विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐनले प्रविधिको क्षेत्रमा पछिल्लो समय आएका थ्रेटको सम्बोधन गर्न नसक्ने अवस्थामा रहेको छ। मुख्यत: प्राइभेसी डाटा प्रोटेक्सन आदि विषयलाई यस विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐनले समेट्न सकेको छैन। यस कारण साइबर कसूर सम्बन्धी नया कानुन बन्नु जरूरी देखिएको छ।

२. **अनुसन्धानमा प्रविधि र विज्ञताको अभाव**: साइबर कसूरको अनुसन्धान गर्ने निकाय नेपाल प्रहरीमा साइवर कसूर सम्बन्धी प्रविधि र विज्ञताको अभाब रहेको छ। यस सम्बन्धमा अनुसन्धान गर्ने निकायको दक्षता पनि निकै कमजोर रहेको अवस्था छ। विकसित देशमा साइबर कसूरको अनुसन्धानमा हाइटेक र इन्टरनेट प्रोटोकलको प्रयोग हुन थालेको छ। नेपाल प्रहरीमा डिजिटल फरेन्सिक ल्याबको स्थापना गरिएको भएता पनि सो को विश्वसनीयता र प्रभावकारी सञ्चालनका लागि आवश्यक दक्षता विकास गर्न सकिएको भने छैन। साइबर कसूरको अनुसन्धानको क्रममा अपनाउनुपर्ने राष्ट्रिय मापदण्डमा अभ्यस्त अनुसन्धान अधिकारीहरूलाई विकास गर्ने तहमा दीर्घकालीन तयारी आज सम्म हुन सकेको छैन। यसको साथै अभियोजनमा संलग्न सरकारी वकिलहरूको क्षमता अभिवृद्धिमा समेत अपेक्षाकृत प्रयासहरू हुन सकेको अवस्था छैन।

३. **साइबर सुरक्षामा संवेदनशीलता**: सरोकारवाला निकायहरूबाट साइबर कसूरसँग सम्बन्धित विषयको सुरक्षाको सम्बन्धमा अपेक्षाकृत संवेदनसिलता अपनाउन सकेको अवस्था छैन।

४. **संस्थागत व्यवस्थाको अभाब**: लामो समय व्यतीत हुँदा पनि विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ मा उल्लिखित प्रावधान अनुरूप सूचना प्रविधि न्यायाधिकरण तथा सूचना प्रविधि पुनरावेदन न्यायाधिकरणको गठन हुन सकेको छैन। नेपालमा प्रयोग गरिने अधिकांश सामाजिक सञ्जालको नियन्त्रण संयन्त्र नेपालसँग छैन। नेपालसँग सामाजिक सञ्जाल माथिको नियन्त्रण या सूचना प्राप्त गर्ने आधिकारिकता नहुँदा साइबर क्राइमको अनुसन्धानमा कठिनाइ देखिएको स्पष्ट छ। साइबर कसूरमा प्रयोग भएका सामाजिक सञ्जालका सम्पर्क कार्यालयहरू नेपालमा नभएको कारणले गर्दा पनि साइबर कसूरको अनुसन्धान र अभियोजनमा चुनौती थपिएको छ।

५. **साइबर कसूर परिभाषित नहुनु**: विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन,२०६३ मा साइबर कसूरको सम्बन्धमा स्पष्ट परिभाषा गरिएको छैन। यस ऐनमा कम्प्युटर सम्बन्धी कसुर भनि कसुरको अपराधीकरण गरिएको छ। यसबाट कम्प्युटर जोडिएको जुनसुकै घटनामा पनि मुद्दा चलाउन सक्ने ठाउँ रहेको देखिन्छ। यसले गर्दा अनुसन्धान

र अभियोजन माग दाबी गोश्वारा प्रकृतिको हुने गरेको छ । विद्युतीय कारोबार सम्बन्धी मुद्दामा प्रहरी अनुसन्धान फितलो हुने गरेको छ । सोही कमजोर अनुसन्धानमा टेकेर अभियोजन हुने हुँदा अधिकांश प्रतिवादीले सफाइ पाउने गरेको तथ्यांक रहेको छ ।

६. **MLA Treaty हुन नसकेको:** विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ ले विद्युतीय कारोबार सम्बन्धी कसूरलाई बहुराष्ट्रिय कसूर (Transnational Crime) को रूपमा रहने भन्ने उल्लेख गरेको छ । यस किसिमको कसूरलाई कानूनी दायरामा ल्याउनको लागि विदेशी राष्ट्रहरूसँग MLA Treaty गर्नु अपरिहार्य छ । लामो समय व्यतीत भइ सक्दा पनि नेपालले MLA Treaty गर्ने सम्बन्धमा कुनै पहल गरेको अवस्था छैन ।

७. **ऐनमा अन्यौलपूर्ण प्रावधान:** विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ को प्रस्तावना र दफा ४७ को प्रावधान बिच एक-आपसमा बेमेल रहेको देखिन्छ । प्रस्तावनामा संस्थागत वा पेशागत बदमासीलाई नियन्त्रण गर्ने आशय उल्लेख गरेको देखिन्छ भने दफा ४७ मा गरिएको उदार र अस्पष्ट व्यवस्थाले गर्दा दुनियावादी विवादमा समेत ऐन लागू भईरहेको अवस्था छ ।

८. **सेवा प्रदायक र प्रयोगकर्ताको सावधानी:** इन्टरनेट सेवाप्रदायक कम्पनीहरूमा पनि साइबर सुरक्षा सम्बन्धी क्षमताको अभाव देखिएको छ । आइसिटी (Information Communication Technology) प्रयोगकर्ताले पनि आत्म सुरक्षाको उपाय नअपनाउँदा थप चुनौती थपिएको छ । यसको कारणबाट साइबर कसूर र सेक्युरिटी थ्रेट बढ्दै गएको छ भने प्राइभेसीमा पनि समस्या आइरहेको छ ।

९. **साइबर कसूरको बढ्दो प्रवृत्ति:** नेपालमा Internet प्रयोगकर्ताको अभिलेख राख्ने प्रणाली छैन । व्यक्तिहरूमा डिजिटल डिभाइसहरूको बढ्दो प्रयोग र मानिसको आपराधिक मानसिकतामा कमी नआएको कारण साइबर कसूर र यसले निम्त्याएको जटिलता समेत बढ्दै गएको छ । यसका साथै सबै सरोकारवाला निकाय, वित्तीय संघसंस्था, उद्योग, शैक्षिक क्षेत्रका साथै सर्वसाधारणमा विद्युतीय कसूर सम्बन्धी सेचतना एवम् जागरूकताको अभाव रहेको छ । व्यक्तिमा साइबर कसूर सम्बन्धी ज्ञानको अभाव, सचेतना तथा जागरूकताको अभाव, कम्प्टयुर प्रयोगकर्ता स्वयंमा सचेतनाको कमीको कारणले गर्दा पनि यस्तो चुनौती झनै बढ्दो मात्रामा रहेको छ ।

१०. **अनुसन्धान र अभियोजनमा थप जटिलता बढेको:** दिन प्रति दिन विश्वमा नयाँ–नयाँ प्रविधिको विकास हुदै गइरहेको छ । सो अनुरूप साइबर कसूर गर्ने शैली र स्वरूपमा पनि परिवर्तन र विस्तार हुने क्रम बढ्दो छ । साइबर कसूरको न्यूनिकरणमा सकृयता उल्लेख्य रूपमा बढ्न सकेको छैन । यी विषयले साइबर कसूरको अनुसन्धान र अभियोजनमा थप जटिलता सिर्जना गरेको छ ।

११. **साइबर सुरक्षाको प्रभावकारी व्यवस्थापन:** नेपालमा साइबर हमलाको अवस्था बढेर गएको हुँदा साइबर कसूरका घटनाहरूमा उल्लेख्य बृद्धि हुदै गइरहेको छ । बैङ्क तथा वित्तिय क्षेत्रमा साइबर कसूरका घटनाहरू बढेर गएको छ । विदेशी एटिएम ह्याकरहरूले नक्कली कार्डबाट पैसा झिकेको घटना पनि बाहिर आएको छ । नेपाली बैंकिङ् क्षेत्रमा साइबर सुरक्षाको अवस्था सन्तोषजनक देखिँदैन । अनलाइन बैंकिङ्ग, मोबाइल बैंकिङ्ग, एसमएस बैंकिङका सुविधा सँगै गम्भीर चुनौती पनि बढ्न थालेको छ । यसअन्तर्गत उपभोक्तालाई झुक्याएर अर्काको रकम आफूले निकाल्ने, एसमएस तथा इमेल फिसिङ्ग गर्ने क्रियाकलापहरू बढेका छन् । तथापि नेपालमा बढ्दो साइबर थ्रेटलाई सम्बोधन गर्नको लागि साइबर सुरक्षाको प्रभावकारी व्यवस्थापन भने हुन सकेको छैन ।

७.२ अध्ययनबाट देखिएका तथ्यका आधारमा गरिएका सुझाबहरु (Recommendations)

विशेषत: विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ विद्युतीय संचार माध्यमबाट हुने कारोबारलाई नियमन र व्यवस्थापन गर्न तर्जुमा गरिएको देखिन्छ । प्रविधिको विकासको विस्फोटनसँगै यससँग सम्बन्धित विभिन्न कसूरहरु पनि सँगसँगै आएका छन् । तसर्थ यी कसूरहरुको नियन्त्रणका लागि विद्युतीय (इलेक्ट्रोनिक) कारोबार कानुनलाई परिमार्जन गरी व्यवस्थित गर्ने र साइबर कसूर अनुसन्धान तथा नियन्त्रण सम्बन्धी छुट्टै कानुन निमार्माण गरी लागु गरिनु पर्ने देखिन्छ । यससँगै साइबर स्पेशको दुनियामा विकास भएका नवीन कसूरको परिभाषा गरी तिनीहरुलाई कसुर कायम गर्दै सजाय गर्ने तर्फ अगाडि बढ्नुपर्ने देखिन्छ । दैनिक रुपमा नवीन प्रवृत्तीहरु भित्रिरहेको सुचनाप्रविधिको विकास र प्रभावकारीताका साथै सुरक्षित बनाई लागु गर्ने सन्दर्भमा निम्न नीतिगत, कानुनी, संरचनागत, कार्यविधिगत सुधारहरु गरिनु पर्दछ ।

माथि उल्लिखित समस्या तथा चुनौतीहरू लाई सम्वोधन गर्नको लागि तल उल्लिखित उपायहरूको अवलम्बन गर्न सकिन्छ ।

७.२.१. कानूनमा सुधार

१. सूचना र प्रविधिको क्षेत्रमा पछिल्लो समय आएको थ्रेटको सम्बोधन गर्न सक्ने खालको साइबर कसूर सम्बन्धी नयाँ कानून जारी गरी कार्यान्वयन गर्नु पर्ने,

२. Digital Evidences लाई कानुनी मान्यता दिनुपर्ने गरि Comprehensive Cyber Law तर्जुमा गर्नुपर्ने,

३. सेल फोन लगायतका Communication service द्वारा Offensive SMS, MMS आदि पठाउनेलाई छुट्टै कारबाहीको व्यवस्थाको कानूनी व्यवस्था गर्नुपर्ने,

४. अनुसन्धानका लागी आवश्यक सूचना तथा कम्प्युटर श्रोतहरूको Monitoring गर्न सक्ने कानूनी ब्यवस्था हुनुपर्ने ।

५. साइबर सुरक्षा र विद्युतीय कारोबार सम्बन्धी छुट्टाछुट्टै कानुन निर्माण गरिनु पर्ने ।

६. कसूर संहिता तथा साइबर कानुनसँग डुप्लीकेशन हुने गरी कानुनहरु बनाउन नहुने । यसरी बनेका कानुनहरु यथाशीघ्र परिमार्जन गरिनुपर्ने ।

७. नेपाल सरकारले तोकेको नियामक निकायले ISP हरुलाई ईन्टरनेट सेवा (Hot-Spot, Free Wi-Fi) प्रयोगकर्ताहरुको अनिवार्य रुपमा फोटो सहितको बिवरण (Contact Details / Subscriber Details) प्रष्ट रुपमा खुल्ने गरी राख्न लगाउने तथा अनुगमन गर्ने व्यवस्था गर्नुपर्ने । साथै उक्त विवरण अनुसन्धानको क्रममा सम्वन्धित निकायबाट माग भई आएमा अनिवार्य उपलब्ध गराउनुपर्ने ।

८. विद्युतीय कारोबार ऐन, २०६३ को दफा ४७ को प्रावधानले "कम्प्युटरसम्बन्धी कसूर" का तत्वहरु अस्पष्ट, अन्योलपूर्ण, विरोधाभाषी रहेको तथा संविधानद्वारा प्रदत्त विचार र अभिव्यक्ति स्वतन्त्रताको अधिकारको सम्मान र संरक्षण हुने गरी कानुन परिमार्जन गर्नुपर्ने ।

९. विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ अन्तर्गत चल्नुपर्ने मुद्दाहरु, कसूर संहिता र प्रतिलिपि अधिकार ऐन, २०५९ बीच स्पष्टता कायम गर्नुपर्ने ।

१०. कानुन कार्यान्वयन गर्ने नियामक निकायहरुलाई नियमन सम्बन्धी पूर्ण अधिकार दिई साधन स्रोत सम्पन्न बनाउनु

पर्ने र निजले दिएको निर्देशनको पालनालाई बाध्यकारी बनाइनु पर्ने ।

११. अधिकाधिक साइबर क्राइम फेसबुक र मोबाइलबाट हुने भएको तथ्याङ्कले देखाएकोले त्यस्ता गतिविधीको नियन्त्रण गर्न साइबर कसूरको नियन्त्रणका क्षेत्रमा भएका कानुनी व्यवस्था विश्लेषण गर्दै ईन्टरनेट (फेसबुक जस्तो सामाजिक संजाल, ईमेल) प्रयोगकर्ताले उक्त प्रविधि अपनाउनुपर्ने नीति निर्देशन र कार्यविधिको पालनाको लागि आवश्यक निर्देशिका, कार्यविधि, मार्गदर्शन बनाई कार्यान्वयन गरिनुपर्ने ।

१२. विद्युतीय कारोबारसम्बन्धी अधिकांश वारदातमा साधनको रुपमा मोबाइल फोन र संजालको रुपमा फेसबुकको प्रयोग हुने गरेकोले साधनको रुपमा कम्प्युटर र ल्यापटप र संजालको रुपमा इमेल (याहु, जिमेल आदि) को प्रयोग गर्ने गरिएको अवस्थालाई प्रमाणमा लिने व्यवस्था कानुनले स्पष्ट गर्नुपर्ने ।

१३. कानुनमा क्लाउड सेवा, डोमिन नाम, साइबर कसूर, सामाजिक संजाल कसूर, इलेक्ट्रोनिक्स डिभाइस लगायत नयाँ नयाँ हार्डवेर र सफ्टवेर सम्बन्धी विद्युतीय औजारको स्पष्ट परिभाषा गरिनु पर्ने ।

१४. नेपालले हालसम्म कुनै पनि देशसँग Mutual Legal Assistance Treaty (MLAT) नगरेको हुँदा विद्युतीय सूचनाको उत्पत्तिकर्ता राष्ट्रसंग नेपालले नियन्त्रणकारी अनुगमनका लागि सुचनाको पहुंच पुर्याउन नसकेकोले सोतर्फ आवश्यक पहल हुनुपर्ने ।

१५. प्रत्यक्ष प्रमाण र परिस्थितीजन्य प्रमाणका अतिरिक्त वैज्ञानिक र वस्तुनिष्ठ प्रमाणका आधारमा कसूरको अनुसन्धान, प्रविधिको उन्नयन र विकासमा लगानी अभिवृद्धि गर्नुपर्ने ।

१६. धेरै जसो मुद्दाहरुमा महिला तथा बालिकाहरु पीडित हुने हुँदा निजहरुको मुद्दालाई गोप्य कार्यविधि अपनाई अनुसन्धान तथा अभियोजन गरिनुपर्ने ।

१७. साइबर कसूरका उजुरीहरु देशभरी पर्ने र हाल साइबर कसूरको मुद्दामा शुरु कारवाही र किनारा गर्ने काम काठमाण्डौं जिल्ला अदालत र पुनरावेदन सुन्ने काम उच्च (साबिकको पुनरावेदन) अदालत पाटनले गर्दै आइरहेकोमा न्यायिक क्षेत्राधिकारको विकेन्द्रीकरण गरिनु पर्ने

१८. कानुनमा तजबिजी सजायको प्रावधान रहेको १ दिनदेखि ५ वर्षसम्म कैद गर्न सकिने र कैद वा जरिवाना वा दुवै सजाय हुने व्यवस्थाले गर्दा एकै खालको कसूरमा पनि फरक फरक मात्रामा सजाय हुने गरेको साथै कसूरको गम्भिरता अनुसार सजाय नहुने गरेकोले कसुरको मात्रा अनुसारको सजाय हुने किसिमले कानुन परिमार्जन गरिनुपर्ने ।

१९. साइबर कानुनमा राष्ट्रिय सुरक्षामा आघात पुग्ने कुरा, विद्युतीय सूचनाको चोरी, ह्याकिङ, क्षति पुर्याउने, साइबर बुलिङ आदि लगायतलाई अपराधिकरण गरिनुपर्ने

२०. सामाजिक संजालको दर्ता र नियमन, सामाजिक संजालमा सम्प्रेषण गर्न नहुने कुराहरु आदि विषयहरु कानुनमा संशोधन गरिनुपर्ने

२१. सूचना प्रविधि न्यायाधिकरण निर्माण गरी पुनरावेदन अदालतका न्यायाधीशलाई त्यसको अध्यक्ष बनाइनु पर्ने साथै यी न्यायाधिकरणहरु प्रदेशमा एउटा रहने गरी स्थापना गरिपर्ने ।

७.२.२. संरचनागत सुधार

१. विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ मा उल्लिखित प्रावधान अनुरूप सूचना प्रविधि न्याधिकरण तथा

सूचना प्रविधि पुनरावेदन न्यायाधिकरणको गठन सम्बन्धमा पहल गर्नु पर्ने,

२. साइबर तथा High Tech Crime हेर्ने छुट्टै Cyber Crime Appellate Tribunal को व्यवस्था गर्नुपर्ने,

३. साइबर सुरक्षा आजको विश्वकै संवेदनशील विषय भएको कारण सार्क, विमस्टेक जस्ता क्षेत्रीय संगठनको माध्यमबाट नेपालले अन्य देशहरू सँगको सहकार्यमा साइबर कसूर घटाउन पहल गर्नु पर्ने।

७.२.३. पारस्परिक कानूनी सहायताको उपयोग

१. Transnational Crime को रूपमा रहेको साइबर कसूरको कसूर र अभियोजनको कार्यमा थप प्रभावकारिता अभिवृद्धिको लागी विदेशी राष्ट्रहरू सँग MLA Treaty गर्ने सम्बन्धमा तयारी थाल्नु पर्ने,

२. साइबर कसूर विदेशमा बसेर समेत गर्न सक्ने प्रकृतिको कसूर भएको हुँदा यसको अनुसन्धान र अभियोजनमा एक मुलुकले अर्को मुलुकको पारस्परिक कानूनी सहायताको जरूरी पर्ने भएको हुँदा यसको लागि राज्यले द्विपक्षिय सन्धीहरू मुलुकहरूसँग विस्तार गर्दै जानु उपयुक्त भएकोले पारस्परिक कानूनी सहायता सम्बन्धी ऐन, २०७० लाई समयानुकुल बनाउदै पारस्परिक कानूनी सहायताको पर्याप्त र उपयूक्त सदुपयोग गर्नु पर्ने।

७.२.४. ल्याव निर्माण र उपयोग

१. प्रहरीमा केन्द्रीय स्तरमा विद्युतीय कसुरसम्बन्धी मुद्दा हेर्न विशिष्टीकृत जनशक्ति र प्रधान कार्यालयमा साइबर फोरेन्सिक ल्याब रहेकोमा प्रदेश तहसम्म सो सुविधा प्रभाबकारी र पर्याप्त मात्रामा विस्तार गर्नुपर्ने।

७.२.५.कसूर अनुसन्धान र अभियोजन

१. संगठित कसूर, आतकंवाद तथा साइबर कसूर नियन्त्रणमा देखिएका चुनौती समाधान गर्न साइबर तथा हाईटेक कसूर अनुसन्धानसम्बन्धी विशेष तालीम प्राप्त गरेको जनशक्तिबाट अनुसन्धान र अभियोजन गर्ने परिपाटी थाल्नुपर्ने।

२. विद्युतीय कसूर गर्ने व्यक्ति विशेष प्राविधिक ज्ञान र क्षमताको प्रयोग गर्ने हुंदा अनुसन्धान र अभियोजन गर्ने व्यक्ति र निकायको भौतिक एवं स्रोत साधनको पर्याप्त व्यवस्थापन गर्नुपर्ने।

३. विद्युतीय बदमासीहरुको नियन्त्रणका लागि देशबीच सूचना र जानकारी आदानप्रदान गर्दै सामूहिक शक्ति लगाउनु पर्ने। सामाजिक सञ्जाललाई आतंकवादीहरुले दुरुपयोग गर्न सक्ने हुंदा यस सम्बन्धमा कानुनी सचेतना र सावधानी अपनाउनु पर्ने।

४. प्रहरीमा केन्द्रीय स्तरमा विद्युतीय कसुरसम्बन्धी मुद्दा हेर्न विशिष्टीकृत जनशक्ति र प्रहरी प्रधान कार्यालयमा साइबरफोरेन्सिक ल्याब रहेता पनि क्षेत्र र जिल्लामा सो सुविधाको अभाव रहेकोले सो विषयमा संगठनात्मक र कार्यात्मक क्षेत्रको विस्तार हुनुपर्ने।

५. विद्युतीय कारोबारसम्बन्धी मुद्दामा प्रहरीद्वारा अनुसन्धान र मागदावी गोश्वारा एवं सोलोडोलो प्रकृतिको हुने गरेकोले सोही कमजोर अनुसन्धानमा टेकेर अभियोजन हुँदा अधिकांश प्रतिवादीले सफाई पाउने गरेको हुंदा प्रत्येक व्याक्तिको कसुरको आधारमा सजाय प्रस्तावित गर्नुपर्ने।

६. साइबर कसूरका बारेमा नागरिकहरुमा चेतना अभिवृद्धिका कार्यक्रमहरु गरिनुपर्ने

७. सामाजिक सञ्जाल प्रयोगकर्ताले अन्जान व्यक्तिलाई साथी नबनाउने, जस्तोसुकै ईमेलको जवाफ नलेख्ने, सामाजिक सञ्जालमा स्टाटस लाईक, सेयर वा कमेन्ट नगर्ने, चरित्र हत्या हुने गरी राखिएको भनाइ वा फोटोहरु सेयर नगर्ने, आफ्नो कम्प्युटर, इमेल आईडी र पासवर्ड अरुलाई दिई चलाउन नदिने जस्ता सामान्य कुराहरुको ख्याल गर्ने कुराहरुको प्रचारप्रसार गरिनुपर्ने।

८. डाटा सेन्टरमा आक्रमण भएमा तुरुन्त त्यसलाई रोक्नका लागि आकस्मिक रुपमा सूचना प्रविधि सहायता समूह निर्माण गरिनु पर्ने।

९. सूचना प्रविधिको कसुरमा अनुसन्धानका लागि र त्यसको मर्मतसंभारका लागि दक्ष जनशक्तिको विकास गरिनुपर्ने।

१०. विद्यालय तहको पाठ्यक्रममा साइबर सुरक्षाको विषयहरु राखिनु पर्ने।

७.२.६. अनुगमन र नियमन

१. नेपाल सरकारले तोकेको नियामक निकायले ISP हरूलाई ईन्टरनेट सेवा प्रयोगकर्ताहरूको अनिवार्य रूपमा फोटो सहितको विवरण प्रष्ट रूपमा खुल्ने गरी राख्न लगाई अनुगमन गर्ने व्यवस्था गर्नुपर्ने,

२. नेपालमा सर्टिफाइड ह्याकिङको कोर्स व्यापक रूपमा विस्तार गरी सरकारी एजेन्सी र कम्पनीहरूमा त्यस्ता जनशक्तिलाई रोजगारीको अवसर दिने तर्फ पहल गर्नु पर्ने,

३. साइबर कसूरमा प्रयोग भएका सामाजिक सञ्जालका सम्पर्क कार्यालयहरूसँग सम्पर्क स्थापित गर्ने र आवश्यक तथ्यांक प्राप्त गर्ने कार्यमा प्रभाबकारीता बृद्धि गर्ने,

४. इन्टरनेट सेवा प्रदायक कम्पनी र प्रयोगकर्ताहरूले इन्टरनेट प्रयोगको सम्बन्धमा पर्याप्त सावधानी अपनाउनु पर्ने,

५. Internet प्रयोगकर्ताको अभिलेख राख्ने प्रणालीको सुरूवात गर्नु पर्ने,

६. बढ्दो साइबर थ्रेटलाई सम्वोधन गर्ने गरी साइबर सुरक्षाको प्रभावकारी व्यवस्थापन गर्नु पर्ने।

७.२.७. क्षमता विकास सम्बन्धमा

१. साइबर कसूरको अनुसन्धान र अभियोजन गर्ने कार्यमा संलग्न जनशक्तिको सीप क्षमता, दक्षतामा सुधार गर्नु पर्ने,

२. साइबर तथा हाईटेक कसूर अनुसन्धान सम्बन्धमा बिदेशमा तालिम तथा अवलोकन भ्रमणको ब्यवस्था गरिनु पर्ने,

३. विद्युतीय कारोबार ऐनको अभिप्राय र सही प्रयोगको सम्बन्धमा प्रहरी र सरकारी वकीलहरूलाई प्राविधिक जानकारीसहितको प्रशिक्षण हरेक तहमा दिइनुपर्ने,

४. अनुसन्धानकर्ता र अभियोजनकर्तालाई प्रयाप्त श्रोत साधनसमेत उपलब्ध गराईनुपर्ने,

५. अनुसन्धान अधिकारी र अभियोजनकर्ता बीचमा विद्युतीय कारोबारको कसुर र अभियोजनमा पारस्परिक सहयोग र सहयात्रीको भावनामा थप समन्वय हुनुपर्ने,

६. अनुसन्धान अधिकारीले अनुसन्धानको प्रक्रियामा प्राविधिक विशेषज्ञको सहजै सहयोग लिनसक्ने व्यवस्था हुनु पर्ने।

७.२.८. प्रचार प्रसार र समन्वय

१. विद्युतीय सामाग्री तथा सेवा र त्यस्तो सेवाको दुरूपयोग गर्दा उत्पन्न हुनसक्ने कानुनी दायित्वका बारेमा व्यापक रूपमा प्रचार प्रसार गर्नु पर्ने,

२. सबै सरोकारवाला निकाय, वित्तिय संघसंस्था, उद्योग, शैक्षिक क्षेत्रका साथै सर्वसाधारणमा विद्युतीय कसूर सम्बन्धी सचेतना एवम् जागरूकता अभिवृद्धि गर्नु पर्ने,

३. सरोकारवाला निकायहरूबाट साइबर कसूरसँग सम्बन्धित विषयको सुरक्षाको सम्बन्धमा संवेदनसिलता अपनाउनु पर्ने।

७.२.९. नागरिक दायित्वमा प्रभावकारीता

१. व्यक्तिले पेनड्राइभ, मेमोरीकार्ड जस्ता डिभाइसको जथाभाबी प्रयोग नगर्ने, शंकास्पद लिङ्क वा चरित्रहत्या गर्ने पोष्टको लाइक शेयर वा ट्याग नगर्ने, आफूले स्टाटस राख्दा सोच विचार गरी राख्ने, विभिन्न प्रलोभन देखाउँदै आएको इमेल नखोल्ने तथा उत्तर पनि नदिने, पासवर्ड पिन कोड वा क्रेडिट कार्ड नम्बर सोधिएमा उत्तर नदिने, परिचितलाई मात्रै साथी बनाउने, व्यक्तिगत जानकारी पोष्ट नगर्ने, कुराकानी गर्दा सदैव सावधान रहने लगायतका सुरक्षाका उपाय अपनाउने,

२. व्यक्तिको तहमा प्रयोगमा रहेको कम्प्युटरमा आधिकारिक लाइसेन्सवाला एन्टिभाइरस इन्स्टल गर्ने, सबै इन्टरनेट खाताहरूमा सजिलै अनुमान गर्न नसकिने पासवर्ड राख्ने र छोटो समयमा नै परिवर्तन गर्ने, महत्वपूर्ण डाटाहरूको ब्याकअप राख्ने, कम्प्युटर अन्यलाई शेयर नगर्ने, इन्टरनेट प्रयोग गरेपछि डिस्कनेक्ट गर्ने तथा सुरक्षित वेवसाइटबाट मात्र अनलाइन सपिङ गर्ने लगायतका सावधानीहरू अपनाउने।

७.२.१०. अन्य सुझावहरू

१. साइबर कसूर भइरहेको स्थानमा तत्काल हस्तक्षेप गर्न Computer Emergency Response Team को समेत व्यवस्था हुनुपर्ने,

२. प्रतिवादी विरूद्ध अभियोगपत्र दायर गर्दा बरामद विद्युतीय सामग्री जफत गर्ने र क्षतिपूर्तिको मागदावी लिने कुरा नछुटाउनेतर्फ सावधानी अपनाउने।

७.३. साइबर सुरक्षा र कसूर सम्बन्धी नयाँ ऐन बनाउनु पर्ने आवश्यकता

सूचना प्रविधिको विकास, प्रबर्द्धन र नियमन गर्न, विद्युतीय अभिलेख तथा डिजिटल हस्ताक्षरको मान्यता, सत्यता र विश्वसनीयतालाई नियमित गर्न, विद्युतीय माध्यमबाट सार्वजनिक सेवा प्रवाह गर्ने सम्बन्धमा साइबर स्पेसमा सङ्कलित, सङ्ग्रहित, प्रशोधित, प्रकाशित वा प्रसारित सूचना, तथ्याङ्क एवम् सूचना तथा सञ्चार प्रविधि प्रणालीको गोपनीयता, अखण्डता, उपलब्धता, प्रमाणिकता र आधिकारिकता कायम राख्न, संवेदनशील सूचना पूर्वाधारको पहिचान तथा सुरक्षा गर्न, सूचना प्रविधि तथा साइबर सुरक्षा सेवा प्रदायकलाई नियमन गर्न र यस क्षेत्रमा हुने कसूर नियन्त्रण गर्ने सम्बन्धमा आवश्यक कानूनी व्यवस्था गर्न मौजुदा विद्युतीय कारोबार ऐन, २०६३ लाई संशोधन र एकीकरण गर्न आवश्यक भएको छ। प्रस्तुत विधेयक तर्जुमा गर्नुपर्ने कारणहरु देहाय बमोजिम रहेका छन् :-

७.३.१. संवैधानिक कारण:

१. नेपालको संविधानको धारा ५१ को "राज्यका नीतिहरू" अन्तर्गत खण्ड (च) को विकास सम्वन्धी नीतिको उपखण्ड (५) र (७) मा उल्लिखित देहायका नीति कार्यान्वयन गर्न सहज हुनेछ।

- "(५) राष्ट्रिय आवश्यकता अनुसार सूचना प्रविधिको विकास र विस्तार गरी त्यसमा सर्वसाधारण जनताको सहज र सरल पहुँच सुनिश्चित गर्ने तथा राष्ट्रिय विकासमा सूचना प्रविधिको उच्चतम उपयोग गर्ने,
- (७) एकीकृत राष्ट्रिय परिचय व्यवस्थापन सूचना प्रणाली विकास गरी नागरिकका सबै प्रकारका सूचना र विवरण एकीकृत रूपमा व्यवस्थापन गर्ने तथा यसलाई राज्यबाट उपलब्ध हुने सेवा सुविधा र राष्ट्रिय विकास योजनासँग आबद्ध गर्ने"

२. धारा २८ वमोजिमको "गोपनियताको हक" लाई विद्युतीय माध्यममा समेत सुनिश्चित गर्न,

३. धारा ४४ बमोजिमको "उपभोक्ताको हक" अन्तर्गत सूचना प्रविधिमा आधारित सेवा तथा व्यापारमा समेत सुनिश्चित गर्न।

७.३.२. अन्तर्राष्ट्रिय दायित्व

According to “UN Resolution ७२/२००, Jan २०१८” Increase the use of information and communications technologies to strengthen good governance.Recognizes the critical importance of private sector investment in information and communications technology infrastructure, content and services and encourage Governments to create legal and regulatory frameworks conducive to increased investment and innovation.

७.३.३.सर्वोच्च अदालतको फैसला

१. सम्मानीत सर्वोच्च अदालतबाट व्यक्तिगत विवरणको गोपनीयता र सूचना सुरक्षण सम्बन्धमा रिट नं. ०६९-WO-०२६८ को मुद्दामा मिति २०७२ माघ २१ गते निर्देशनात्मक आदेश जारी भएको।

२. सर्वोच्च अदालतले नेपाली नागरिकको डाटा नेपाल सरकारको नियन्त्रणमा रहन तथा विदेशीको हातमा नजाने व्यवस्था मिलाउन मिति २०७४।०१।१० मा भएको अन्तरिम आदेशलाई मिति २०७४।०१।२५ को आदेशले (०७३-WO-१०९७) निरन्तरता दिएकोले डाटाको सुरक्षा विषयको गाम्भिर्यता पुष्टि भएको।

७.३.४.सरकारको नीति तथा कार्यक्रम

१. साइबर सुरक्षा सम्बन्धि राष्ट्रिय नीति, २०८०

२. सूचना तथा सञ्चार प्रविधि नीति, २०७२ को "११.१ सूचना तथा सञ्चार प्रविधिमा पहुँच माध्यम वा विषयवस्तु विकास " शिर्षक अन्तरगत निम्न नीति उल्लेख भएको छ:-

विकास एवं सार्वजनिक सेवा प्रवाह सम्वन्धी चुनौति सामना गर्न सूचना तथा प्रविधिमा आधारित नवीनतम तथा मौलिक प्रयोग प्रवर्द्धन गर्न विषेश कार्यक्रम (Innovative Use) लागु गरिनेछ।

३. सूचना तथा सञ्चार प्रविधि नीति, २०७२ को "११.६ सूचना तथा सञ्चार प्रविधि सम्बन्धी उद्योग क्षेत्रको विकास" शिर्षक अन्तरगत निम्न नीति उल्लेख भएको छ:-

अन्तराष्ट्रिय स्तरमा प्रतिस्पर्धा गर्न सक्ने सूचना तथा सञ्चार उद्योग क्षेत्रको विकास गर्न विशेष कार्यक्रम तर्जुमा गरी लागु गरिनेछ । सूचना तथा सञ्चार प्रविधिका क्षेत्रमा विदेशी श्रोत समेतको परिचालन गरी लागु गरिने परियोजनामा स्वदेशी व्यवसायीहरुलाई सहभागी हुने वातावरण निर्माण गरिनेछ ।

४. सूचना तथा सञ्चार प्रविधि नीति, २०७२ को "११.१७ सुशासन तथा सार्वजनिक सेवा प्रवाहमा सूचना तथा सञ्चार प्रविधि" शिर्षक अन्तरगत निम्न नीति उल्लेख भएको छ:-

सूचना तथा सञ्चार प्रविधिको प्रयोगद्वारा सार्वजनिक सेवा प्रवाहलाई प्रभावकारी बनाउने विद्यमान प्रयासहरुलाई निरन्तरता दिइनेछ ।

५. नेपाल सरकारको आ.व. २०८०/८१ को नीति तथा कार्यक्रममा देहाय वमोजिमका कार्यक्रमहरु रहेको छ:

सञ्चार तथा सूचना प्रविधिको प्रयोगमा आम नागरिकको पहुँच अभिवृद्धि गरिनेछ। शिक्षा स्वास्थ्य विकास निर्माण र सेवा प्रवाह लगायतका क्षेत्रमा सूचना प्रविधिको प्रयोगलाई विस्तार गरिनेछ । ज्ञानमा आधारित अर्थतन्त्रको विकास र सुशासनका लागि सूचना प्रविधि प्रणालीको अनुसन्धान, विकास र विस्तार गरिनेछ ।

सरकारी निकायबाट सञ्चालित अनलाइन प्रणालीहरुबीच अन्तरआबद्धता कायम गरी सेवा उपलब्ध गराइनेछ । अनलाइन सेवाहरु वडा तह सम्म नै उपलब्ध गराइनेछ । विद्युतीय प्रणालीबीच तथ्याङ्क आदन प्रदान गर्न डाटा एक्सचेन्ज प्लेटफर्म निर्माण गरिनेछ ।

राष्ट्रिय साइबर सुरक्षा केन्द्र सञ्चालनमा ल्याई साइबर सुरक्षाजन्य जोखिमलाई न्यूनीकरण गरिनेछ ।

७.४. नयाँ ऐन बनाई कार्यान्वयन भए पश्चात हासिल गरिने उपलब्धि

- विद्युतीय शासनको अवधारणा प्रभावकारी रुपमा कार्यान्वयन हुन कानूनी आधार तय हुनेछ ।
- विद्युतीय अभिलेखलाई कानूनी मान्यता दिनेछ ।
- सूचना प्रविधि सम्बन्धी व्यवसायहरु व्यवस्थित, नियमित तथा मर्यादित भई यस क्षेत्रमा वैदेशिक लगानी वृद्दि हुनेछ ।
- नेपालमा विद्युतीय स्वरुपमा रहेको सूचना सूरक्षा, संरक्षण तथा वैयक्तिक विवरणको गोपनीयताको स्तरमा उल्लेखनीय वृद्दि हुनेछ ।

७.५. प्रस्तावित कानूनमा समावेश हुनु पर्ने न्यूनतम विषय

- हालको विद्युतीय कारोबार ऐनमा रहेको विद्युतीय कारोवार तथा डिजिटल हस्ताक्षर सम्बन्धी प्रावधानलाई समयानुसार अध्यावधिक गरी समावेश गरिने,

- विद्युतीय शासन सम्बन्धी प्रावधानहरु,
- डोमेन नाम दर्ता तथा व्यवस्थापन सम्बन्धी प्रावधानहरु,
- सूचना प्रविधि व्यवसाय सम्बन्धी प्रावधानहरु,
- सूचना प्रविधिको क्षेत्रमा जनशक्तिको क्षमता विकास सम्बन्धी व्यवस्था,
- सूचना सुरक्षा सम्बन्धी प्रावधानहरु,
- सेवा प्रदायक सम्बन्धी प्रावधानहरु,
- साइबर सुरक्षा केन्द्र सम्बन्धी व्यवस्था,
- साइबर सुरक्षा परीक्षण र परीक्षक सम्बन्धी व्यवस्था,
- साइबर सुरक्षा सेवा प्रदान गर्न अनुमतिपत्र लिनुपर्ने व्यवस्था,
- सूचना सुरक्षा सम्बन्धी व्यवस्था,
- हालको विद्युतीय कारोबार ऐनमा रहेको कसूर तथा सजाय, अनुसन्धान, अभियोजन, मुद्दा हेर्ने र पुनरावेदन सुन्ने सम्बन्धी समयसापेक्ष प्रावधान राखी कसुरको परिभाषालाई समेत थप स्पष्ट रुपमा व्याख्या गरिने,
- विद्युतीय कसुरको प्रमाण संकलन सम्बन्धी प्रावधानहरु थप गरिने,

७.६.निष्कर्ष (Conclusion)

नेपालमा साइबर कसूर सम्बन्धी कसुरमा विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ को आधारमा अनुसन्धान र अभियोजन हुँदै आएको छ। विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ को परिच्छेद ९ मा उल्लिखित कम्प्युटर सम्बन्धी कसुरहरूलाई नै साइबर कसूरको रूपमा अनुसन्धान र अभियोजनको कार्य हुँदै आएको पाइन्छ। पछिल्लो समयमा सूचना र प्रविधिको क्षेत्रमा भएको व्यापक विस्तार र प्रयोगको कारण साइबर कसूरको प्रवृत्ति, शैली र मोडस अपरेण्डी (Modus Operandi) मा पनि व्यापक परिवर्तन भएको छ। साइबर कसूरको क्षेत्रमा देखा परेको यस किसिमको परिवर्तनलाई विद्यमान विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ ले सम्बोधन गर्न नसकेको भनि नया साइबर कानूनको निर्माण हुनु पर्ने भन्ने सरोकारवालाहरूको माग पनि बढ्न थालेको छ। सूचना र प्रविधिमा रहेको परिवर्तनको कारण यसको अनुसन्धान र अभियोजनमा पनि बिभिन्न चुनौतीको सामना गर्नु परेको अवस्था रहेको छ। विशेष गरी साइबर कसूरको स्पष्ट परिभाषाको अभाब रहेको, अनुसन्धान र अभियोजनको कार्यमा दक्षता अभिवृद्धि हुन नसकेको, साइबर कसूरको बढ्दो अवस्था, साइबर सुरक्षाको कमजोर अवस्था आदीलाई मुख्य चुनौतीको रूपमा लिन सकिन्छ। यी चुनौतीहरूलाई सामना गर्दै साइबर कसूरको अनुसन्धान र अभियोजनलाई प्रभाबकारी बनाइ न्याय सम्पादन कार्यलाई सहयोग पुर्‍याउनु आजको आवश्यकता हो। सूचना प्रविधिको विकासमा कम्युटरले महत्वपुर्ण भूमिका खेलेको पाइन्छ। यसको माध्यमबाट सूचना सम्प्रेषण गर्ने देखि लिएर मानिसको आवश्यकता अनुसारका सबै कार्य छिटो छरितो र गुणस्तरीय रुपमा सम्पादन गर्न सघाउ पुर्याउँदै आएको छ। अहिले हरेक व्यक्ति कम्प्युटर प्रणालीबाट बाहिर छैन। मोबाइल, ल्यापटप, डेक्सटप कम्युटर, ट्याबलेट लगायत कुनै न कुनै रुपमा सबै व्यक्तिहरु कम्प्युटरमा जोडिएका छन्। यस सँगसँगै कम्प्युटरसँग सम्बन्धित कसूरहरु पनि बढिरहेका छन्। यी कसूरहरुको नियन्त्रण पेचिलो बनेको छ। नेपालमा विद्युतीय कसूरको नियन्त्रणका लागि विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ कार्यान्वयनमा रहेको छ।

२०६३ सालमा आएको विद्युतीय कारोबार ऐनले अभिलेख तथा डिजिटल हस्ताक्षरसम्बन्धी व्यवस्था अन्तर्गत यसले विद्युतीय अभिलेखको प्रमाणिकता, विद्युतीय अभिलेख र डिजिटल हस्ताक्षरको कानुनी मान्यता, सुरक्षित विद्युतीय अभिलेख, सुरक्षित डिजिटल हस्ताक्षरसम्बन्धी व्यवस्थाहरू गरेको छ। त्यसैगरी विद्युतीय अभिलेखको सम्प्रेषण, प्राप्ति र स्वीकार, नियन्त्रण तथा प्रमाणीकरण गर्ने निकायसम्बन्धी व्यवस्था, डिजिटल हस्ताक्षर तथा प्रमाणसम्बन्धी व्यवस्था, ग्राहकको काम कर्तव्य र अधिकार, विद्युतीय अभिलेख र डिजिटल हस्ताक्षरको सरकारी प्रयोग, नेटवर्क सेवासम्बन्धी व्यवस्थाहरू गरेको छ भने उल्लिखित व्यवस्थाहरू उल्लंघन गर्ने वा निषेधित कार्यउपर सजायको निर्धारण समेत गरिएको छ। जसमा कम्प्युटर स्रोत संकेतको चोरी, नष्ट वा परिवर्तन गर्न, कम्प्युटर सामग्रीमा अनधिकृत पहुँच, कम्प्युटर सूचना प्रणालीमा क्षति, विद्युतीय स्वरूपमा गैरकानुनी कुरा प्रकाशन, गोपनीयता भंग, झुट्ठा बेहोराको सूचना, झुट्ठा इजाजतपत्र वा प्रमाणपत्र पेस गर्ने वा देखाउने, तोकिएको विवरण वा कागजात दाखिला नगर्ने, कम्प्युटर जालसाजी, कम्प्युटरसम्बन्धी कसूर गर्न दुरुत्साहन, मतियारलगायतका कार्यउपर सजाय गरिन्छ भने अन्य कार्यमा सजाय गर्न सकिँदैन।

साइबर कसूर कम्प्युटर तथा कम्प्युटर नेटवर्क प्रयोग गरेर हुने जुनसुकै प्रकारका कसूरहरु हुन्। यसमा इन्टरनेट, इन्ट्रानेट र एक्स्ट्रानेटसँग सम्बन्धित आपराधिक गतिविधिहरु पर्छन्। भौतिक बल प्रयोगबिना कम्प्युटर प्रविधि र इन्टरनेटको प्रयोगद्वारा पीडितको इच्छा र चाहना विपरीत साइबर स्पेसलाई प्रभावमा पारी सूचनाको सृजना, वितरण, फेरबदल, चोरी, दुरुपयोग र नष्ट गर्ने कार्य आदी पर्छन्। नेपालमा विद्युतीय कारोबार ऐन र फौजदारी कसूर संहिताले साइबर कसूरलाई समेट्न नसकेकाले यसलाई सम्बोधन गर्न छुट्टै साइबर कानुन जरुरी देखिन्छ। पछिल्ला केही घटनाहरु हेर्ने हो भने नेपालको साइबर स्पेस खतरामा छ । देश विदेशबाट नेपालको साइबर स्पेसमा कम्प्युटर, मोबाइल र यसका विभिन्न नेटवर्कबाट आक्रमण हुने क्रम रोकिएको छैन । सरकार, दूरसञ्चार र इन्टरनेट सेवा प्रदायक, बैंक, एयरलाइन्स लगायतका कम्पनीका सिष्टममा लगातार आक्रमण भइरहेका छन् । यद्यपी सबै घटना बाहिर आएका छैनन्। हाम्रो साइबर सेक्युरिटीको संरचना कमजोर भएकाले जोखिम निम्तिएको छ तरपनि यतातर्फ सरोकारवालाको ध्यान आउन सकेको देखिँदैन।

विद्युतीय उपकरणहरु कम्प्युटर, मोबाइल, तथा यसको नेटवर्कका माध्यमबाट हुने कुनै पनि प्रकारका अपराधिक कार्यलाई साइबर कसूर मानिन्छ । इन्टरनेटको प्रयोगमार्फत गरिने चरित्र हत्या, हिंसा फैलाउने कार्य, यौनजन्य हिंसा, इण्टरनेट फ्रड, अर्काको पहिचान अनाधिकृत रूपमा प्रयोग, क्रेडिट कार्ड तथा एकाउण्ट आदिको चोरी गरी गरिने बैङ्किङ कसुर, अर्काको कम्प्युटर, विद्युतीय उपकरण तथा नेटवर्कमा पुर्याइउने क्षति लगायत अवैधानिक कार्यलाई पनि विश्वका अधिकांश मुलुकका कानूनले साइबर कसूर मानेको छ । साइबर क्राइमलाई सम्बोधन गर्न अन्तराष्ट्रिय एवं क्षेत्रीयगत रुपमा विभिन्न कानून बनेका छन् । संयुक्त राष्ट्र संघ, अन्तर्राष्ट्रिय दूरसञ्चार युनियन, युरोपियन युनियन लगायतले आफ्ना सदस्य राष्ट्रका लागि साइबर कसूर विरुद्ध ऐन र नियम ल्याइरहेका छन् । विद्युतीय कारोबार ऐन र फौजदारी कसूर संहिताले साइबर कसूरलाई समेट्न नसकेकाले यसलाई सम्बोधन गर्न छुट्टै साइबर कानुन जरुरी छ। ऐन कानुनमा सामयिक परिमार्जन, क्षमता विकास, ऐनको कार्यान्वयन र अभ्यासका बारेमा अध्ययन अनुसन्धान, पुर्वाधारको विकास, अबधारणाको स्पष्टता लगायत नवीन प्रविधिसँगसँगै जनशक्तिको विकास भएमा समृद्ध समाजको निर्माण गर्न सकिन्छ।

सन्दर्भ सामाग्री

१. मानव अधिकारको विश्वव्यापी घोषणापत्र, १९४८

२. नागरिक तथा राजनीतिक अधिकारसम्बन्धी अन्तर्राष्ट्रिय अनुबन्ध, १९६६

३. UNCITRAL Model Law on Electronic Commerce (१९९६)

४. Budapest Convention on Cyber Crime, European Treaty Series - No. १८५

५. UNCITRAL Model Law on Electronic Signatures (२००१)

६. नेपालको संविधान, धारा १६

७. विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३, दफा ४४

८. मुलुकी अपराध संहिता, २०७४, दफा २९३

९. विद्युतीय कारोबार नियमावली, २०६४

१०. राष्ट्रिय साइबर सुरक्षा नीति, २०७३

११. सर्वोच्च अदालतबाट प्रतिपादित नजिरहरू

o निर्णय नं. ९४३५ परमादेश

o निर्णय नं. ९६२१ - जिउ मास्ने बेच्ने

१२. प्रतिपादन (२०७३), पृष्ठ १–१७, राष्ट्रिय न्यायिक प्रतिष्ठान, काठमाडौं

१३. नेपाल कानून परिचर्चा (२०७७) नेपाल ल क्याम्पस, काठमाडौ

१४. Websites हरू

o https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-१२-types-of-cyber-crime.html

o file:///C:/Users/user/Downloads/३१९-१३-२२३१-१-१०-२०२००१२१.pdf

o file:///C:/Users/user/Downloads/३१९-१३-२२३१-१-१०-२०२००१२१.pdf

o https://www.oas.org/juridico/spanish/us_cyb_laws.pdf

o https://securelist.com/cybercrime-and-the-law-a-review-of-uk-computer-crime-legislation/३६२५३/

o https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf

अनुसूची १

अभियोजन तथा फैसलाका सुचकहरु

- पीडितको उमेर..... प्रतिवादीको उमेर.....
- पीडितको लिङ्ग ..... प्रतिवादीको लिङ्ग.....
- कसूर गर्न प्रयोग गरिएको प्रविधी

• मोबाईल ल्यापटप कम्प्यूटर ट्याबलेट अन्य

- उक्त कसूर सामाजिक संजाल प्रयोग गरी गरिएको हो?

• हो
होईन

- सामाजिक संजालबाट हो भने कुन सामाजिक संजाल प्रयोग गरिएको हो?

• फेसबुक टिकटक ह्वाट्सएप ट्विटर भाईबर अन्य

- पीडितको प्रतिवादीसँग सम्बन्ध

• छिमेकी सँगै काम गर्ने चिनजान नचिनेको

- प्रतिवादीको पेश व्यवसायः
- वारदातको समयमा प्रतिवादी रहेको स्थानः

• देश भित्र
देश बाहिर

- साइबर कसूरको प्रकृती

• Cyber Enabled Cyber Assisted

- कसूरको उद्देश्य

• आर्थिक उपार्जन यौन दुर्व्यवहार मनोरञ्जन
अन्य.....

- वारदात भएको कती समय पछी जाहेरी परेकोः.....
- अपराधको सूचनाको माध्यमः

• प्रत्यक्ष हुलाक मार्फत सरकारी वकील मार्फत एप मार्फत अन्य

- कसूरमा प्रयोग भएको User ID फेक भए नभएको .....
- जाहेरी दरखास्त प्रहरी कार्यालयले दर्ता नगरेको उपरको उजुरी परे नपरेको.....
- अनुसन्धानमा निर्देशन दिएको संख्याः .....
- म्याद थपको निवेदनमा आधार कारण खुलाउने गरेको/ नगरेको?

- मुद्दामा अनुसन्धानको शुरू चरणदेखि नै सरकारी वकील तोक्ने गरेको वा नगरेको?.....
- दावीको दफा.....
- प्रमाण खुलाई प्रतिवादी पिच्छे दावी (Per Capita Prosecution) लिने गरेको वा नगरेको?
- मागदावी लिनु पर्ने सवै कुराको कानूनको दफा खुलाई दावी लिएको वा नलिइएको?
- पटकेको मागदावी रहे नरहेको,
- क्षतिपूर्तिको दावी लिए नलिएको,
- सजाय छुटको दावी लिए नलिएको,
- जाहेरी दर्ता र अभियोग पत्र दर्ता बीचको समयावधि.....
- सुरुदेखि तोकिएको सरकारी वकीलले अभियोजन गरेको वा नगरेको?
- प्रतिवादी पक्राउ परे/नपरेको अवस्था
- मौकाको बयानको अवस्था
  - सावितीइन्कारी
- प्रतिवादीको अदालतमा भएको बयानको अवस्था
  - सावितीइन्कारी
- थुनछेक आदेशको अवस्था
  - साधारण तारेखमा राख्नेधरौट वा बैंक जमानतमा छाड्नेथुनामा राख्ने
- जाहेरवाला/पीडितको वकपत्रको अवस्था
- जाहेरी अनुसार (अनुकुल बकपत्र)जाहेरीको प्रतिकुल
- सजायपूर्वको प्रतिवेदनको अवस्था
  - पेश भएकोपेश नभएकोपेश भए नभएको बिषय फैसलामा नखुलेको
- फैसला हुन लागेको समय……..
- कसूर ठहर
  - भएकोनभएकोआंशिक
- अभियोग मागदाबी बमोजिम
  - कसूर ठहरआंशिकसफाईमुल्तवी
- कानूनको अभावमा फैसलामा अभियोगदावी बमोजिम कसूर ठहर हुन नसकेको अवस्था रहे नरहेको?.....
- सजाय
  - कैद ……जरिवाना .....दुवै
- एकीकृत सजाय
  - भएकोनभएको

- पटकेको तर्फ सजाय (पटके मागदावी भएकोमा मात्र)
  - भएको नदिएको
- क्षतिपूर्ति
  - दिएको नदिएको
- क्षतिपूर्ति रकम

  .....
- अन्तरिम क्षतिपूर्ति दिएको नदिएको