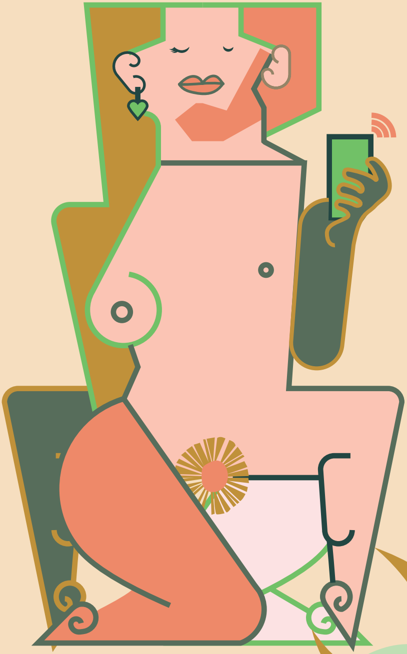
लैंगिकता, प्रविधि र यौनिकता

हाते पुस्तिका



लुम, २०२०

लेखकः पुष्पा जोशी

सम्पादकः बिनु सुवेदी

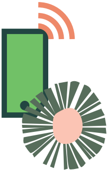
सल्लाहकारः क्षितिज अधिराज

लूम
१४२, पञ्चायन मार्ग
थापाथली, काठमाडौं ,नेपाल
टेलिफोन नं.: ९७७–४२५१३३५, ४२५१७०९
इमेलः loom@loomnepal.org
वेबसाइटः www.taannepal.org.np
ISBN: 978-9937-0-5874-2

लैंगिकता, प्रविधि र यौनिकता

केहि दशक यता इन्टरनेटले मानव जीवनमा ठूलो परिवर्तन ल्याएको छ । इन्टरनेट मार्फत् हामीले अझै धेरै स्वतन्त्रताको अनुभूती गर्न सकेका छौं । हाम्रो अभिव्यक्ति गर्ने ठाउँ फराकिलो भएको छ । हामीले संसारका हरेक कुनामा रहेका व्यक्तिहरूसँग सञ्चार गर्न मिल्ने, सूचना आदानप्रदान गर्न मिल्ने भएको छ ।

अनुसन्धानका अनुसार इन्टरनेटले महिलालाई आत्मनिर्णयको स्वतन्त्रता प्रदान गरेको छ । सामाजिक सञ्जालमार्फत महिलाहरूले आफूलाई फरक ढङ्गबाट प्रस्तुत गर्न सक्ने भएका छन् । समाजले तोकिदिएको दायरालाई चिर्दै आफ्नो अभिव्यक्ति राख्न सक्ने भएका छन् । प्रेम सम्वन्धहरू बिस्तार गर्न सक्ने भएका छन् । विभिन्न विषय र सूचनामा पहुँच पुगेको छ । महिलाहरूका लागि इन्टरनेट आफ्नो यौनिकतामा रमाउने थलो पनि बनेको छ ।



भौतिक संसारमा महिला र यौन अल्पसंख्यक व्यक्तिहरुलाई जतिको गाह्रो छ, पहुँच र प्रयोगको आधारमा उनीहरुलाई इन्टरनेटमा पनि उत्तिकै गाह्रो छ। प्रविधिबाट नयाँ सूचनासँग परिचित हुन सकिने भएकाले प्रविधिलाई एक शक्तिको स्वरूप मान्न सकिन्छ ।

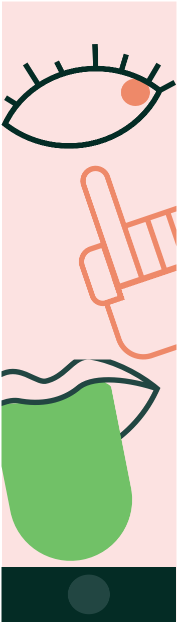
यद्यपी, इन्टरनेट र प्रविधि, लैंगिकताको विषयले प्रभावित छ । भौतिक संसारमा महिला र यौन अल्पसङ्ख्यक व्यक्तिहरूलाई जति गाह्रो छ, इन्टरनेटमा पहुँच र यसको प्रयोगमा पनि उनीहरूलाई उत्तिकै गाह्रो छ । प्रविधिबाट आफ्नो ज्ञानको क्षितिज फराकिलो गर्न मिल्ने र नयाँ सूचनाहरूका बारेमा जानकार हुन सकिने हुँदा यसलाई शक्तिको स्वरूमा लिन सकिन्छ । तसर्थ, महिला र यौन अल्पसङ्ख्यक व्यक्तिहरूलाई यिनै विभिन्न संरचनागत विभेदका कारणले इन्टरनेट र प्रविधिमा पहुँच गर्न गाह्रो भएको हो । पछिल्लो समयमा इन्टरनेटमार्फत् हुने वा अनलाइन लैंगिक हिंसा पनि एक प्रमुख समस्या बन्दै आएको छ ।

१. अनलाइन हिंसा

भौतिक संसारमा हुने भेदभाव र हिंसाले अनलाइन संसारमा पनि निरन्तरता पाएको छ । किनभने अनलाइन संसारमा पनि भौतिक संसारमा भएकै व्यक्तिहरू प्रयोगकर्ताका रूपमा छन् । त्यसकारण अनलाइन हिंसा कुनै नयाँ प्रकारको हिंसा होइन । यो त भौतिक संसारमा हुने विभेदकै निरन्तरता हो; जसमा इन्टरनेटलाई एउटा माध्यमका रूपमा प्रयोग गरिन्छ ।

लैंगिकताका आधारमा हुने अनलाइन हिंसाका केही प्रकारहरू:

अनलाइनमा हुने हिंसा, जुन व्यक्तिको शरीर, यौनिकता, लैंगिकता, यौन अभिमूखिकरण आदिलाई लक्षित गरेर गरिएको हुन्छ । त्यसप्रकारको हिंसालाई लैंगिकताका आधारमा हुने अनलाइन हिंसा भनिन्छ । त्यस्ता केही हिंसाहरूलाई तल विस्तृत रूपमा व्यारव्या गरिएको छ ।



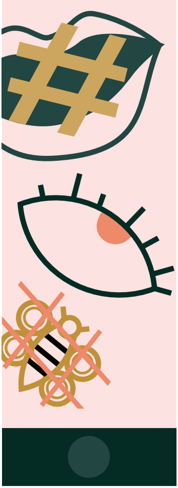
हिंसाका केहि प्रकारहरू:

(क) पहिचानको चोरी अर्थात् आइडेन्टिटी थेफ्ट (Identity theft/Impersonation): कुनै व्यक्तिको पहिचान वा आइडेन्टिटीमा उक्त व्यक्तिलाई नै थाहा नहुने गरि इन्टरनेटको कुनै पनि प्लेटफर्म जस्तैः फेसबुक, ट्वीटर, इन्स्टग्राम आदिमा अकाउन्ट बनाउनुलाई पहिचानको चोरी अर्थात् आइडेन्टिटी थेफ्ट भनिन्छ ।

(ख) डोक्सिङ (Doxing): कुनै पनि मानिसको व्यक्तिगत र गोप्य सूचना उसको अनुमति विना इन्टरनेटमा प्रकाशन गर्नुलाई डोक्सिङ भनिन्छ ।

(ग) अकाउन्ट कम्प्रोमाइज (Account Compromise): इन्टरनेटको कुनै पनि सामाजिक सञ्जाल जस्तैः फेसबुक, ट्वीटर आदिमा उक्त प्लेटफर्ममा अकाउन्ट भएको व्यक्तिको अकाउन्ट गुम्नु वा ह्याक हुनुलाई अकाउन्ट कम्प्रोमाइज भनिन्छ ।

(घ) धम्की (Blackmail) र सेक्सटोर्सन (Sextortion): कुनै पनि व्यक्तिको गोप्य र व्यक्तिगत सूचना खुलाई दिन्छु भन्दै पैसा वा अरु कुराको माग गर्नुलाई धम्की वा Blackmail भनिन्छ ।



पैसा वा अरु वस्तुको सट्टामा यौन सम्पर्कको माग गरिनुलाई सेक्सटोर्सन भनिन्छ ।

(ङ) रिभेन्ज पोर्न (Revenge Porn): अनुमति लिएर वा नलिकनै खिचिएको यौन सम्पर्कको भिडियोलाई बदला लिने नियतले इन्टरनेट प्लेटफर्महरूमा प्रकाशन गर्नुलाई रिभेन्ज पोर्न भनिन्छ ।

(च) साइबर स्टकिङ (Cyber Stalking): कुनै पनि व्यक्तिलाई इन्टरनेटमा पछ्याउनुलाई साइबर स्टकिङ भनिन्छ । उदाहरणका लागि तपाईको एक वर्ष अगाडीका पोष्टहरूमा कुनै पनि व्यक्तिको लाइक/कमेन्ट आउनु, जसले तपाईंलाई अप्ठ्यारो महसुस हुनुका साथै मानसिक तनाव पनि हुनसक्छ ।

(छ) आउटिङ (Outing): कुनै पनि व्यक्तिको अनुमति बिना उक्त व्यक्तिको लैंगिक पहिचान वा यौन अभिमूखिकरण इन्टरनेटमार्फत् बाहिर ल्याउनुलाई आउटिङ भनिन्छ ।

(ज) हनी ट्र्याप (Honey Trap): इन्टरनेट प्लेटफर्ममार्फत् कसैको विश्वास जित्नु र उक्त व्यक्तिलाई धोका दिनुलाई हनी ट्र्याप भनिन्छ । उदाहरणका लागि समलिंगी सम्बन्ध गैरकानुनी भएको देशमा कुनै प्रहरीले आफू समलिंगी हुँ भनी अर्को समलिंगीको विश्वास जिती, उक्त व्यक्तिलाई भेट्न बोलाएर पक्राउ गर्नुलाई हनी ट्र्याप भन्न सकिन्छ ।

(झ) ट्रोलिङ (Trooling): कुनै व्यक्ति वा समुदायको पहिचानमा आँच आउने गरी कुनै अनलाइन विषयवस्तु (पोष्टर, ग्राफिक, टेक्स्ट आदि) प्रकाशन गर्नुलाई ट्रोलिङ भनिन्छ ।

(ञ) हेट स्पीज (Hate Spech): कुनै समुदाय वा व्यक्तिको आत्मसम्मानमा आँच आउने गरी प्लेटफर्ममा गालीगलौज, अपमान, आरोप, धम्की दिनुलाई हेट स्पीज भनिन्छ ।

२. के-कस्ता गतिविधिले तपाईंलाई धेरै जोखिम हुन सक्छ?

(क) तपाईंको पासवर्ड अरु कसैलाई थाहा छ भने वा तपाईंले आफ्नो पासवर्ड अरु कसैलाई दिनु भएको छ भने,

(ख) यदि तपाईंले आफ्नो Geolocation सधैंभरि अन राख्नु भएको छ भने,

(ग) यदि तपाईंले आफ्नो घरको ठेगाना सामाजिक सञ्जालमा राख्नु भएको छ भने,

(घ) यदि तपाईंले आफ्नो विद्युत्तिय यन्त्र जस्तैः कम्प्युटर, ट्यावलेट, मोबाइल आदिमा पासवर्ड राख्नु भएको छैन भने ।

३. इन्टरनेट प्रयोग गर्दा अनुमतिको महत्व

भौतिक संसारमा जस्तै अनलाइन संसारमा पनि अनुमतिको उत्तिकै महत्व हुन्छ । कुनै पनि व्यक्तिको व्यक्तिगत सुरक्षा र आत्मसम्मानका लागि हामीले व्यक्तिको अनुमतिको कदर गर्नुपर्छ । कुनै पनि व्यक्तिको फोटो खिच्नु भन्दा अगाडि उक्त व्यक्तिको अनुमति लिनु पर्दछ । उक्त फोटो कहाँ कुन रूपले प्रयोग गर्दै हुनुहुन्छ सो व्यक्तिलाई स्पष्ट जानकारी दिनु पर्दछ ।

यदि सो व्यक्तिले आफू उपस्थित भएको फोटो वा भिडियो पहिले नै प्रयोग गर्न अनुमति दिएता पनि सो व्यक्तिले कुनै पनि बेला आफ्नो अनुमति फिर्ता लिन सक्छ । यसरी हामीले एकअर्काको अनुमतिको सम्मान, भौतिक र अनलाइन संसार दुवैमा गर्न सक्छौं । यदि इन्टरनेटको प्रयोग गर्दा अनुमतिको सम्मान गरिएन भने उक्त डिजिटल विषयवस्तुमा भएको व्यक्तिहरूको सुरक्षा र आत्मसम्मानमा ठूलो क्षति पुग्नसक्छ ।

४. सामाजिक सञ्जाललाई अभियानको हिस्सा कसरी बनाउन सकिन्छ?

इन्टरनेट प्रयोगकर्ताहरू माझ लोकप्रिय सामाजिक सञ्जालले बालकदेखि वृद्धसम्म, व्यापारीदेखि अभियन्ता सबैलाई आकर्षित गरेको छ । अहिले फेसबुक, इन्स्टाग्राम, ट्वीटरमार्फत संसारभरका मानिसहरू जोडिएका छन् । फेसबुकका अनुसार नेपालमा मात्रै साठी लाखभन्दा धेरै फेसबुक प्रयोगकर्ताहरु छन् । त्यसकारण पनि कुनै पनि अभियानका लागि सामाजिक सञ्जाल एक उपयुक्त र प्रभावकारी स्थान वा माध्यम हुनसक्छ । 'बालुवाटार ओगटौं', 'निर्मला हत्याकाण्ड' आदि अभियानमा सामाजिक सञ्जालले निकै ठूलो भूमिका निर्वाह गरेको थियो । त्यसैगरी राष्ट्रिय तथा अन्तर्राष्ट्रिय स्तरमा त्यस्ता थुप्रै उदाहरणहरु छन्, जसमा सामाजिक सञ्जालले अभियानलाई वृहत रूप दिन मद्दत गरेको छ ।

अभियानका लागि सामाजिक सञ्जालको सुरक्षित प्रयोग निम्न लिखित तरिकाले गर्न सकिन्छः

- कुनै पनि दुईवटा सामाजिक सञ्जाल एकअर्कासँग आवद्ध नहुँदा राम्रो हुन्छ ।
- छुट्टाछुट्टै सामाजिक सञ्जालमा छुट्टाछुट्टै पासवर्ड हाल्नुहोस् ।
- सार्वजनिक वाईफाईमा आफ्नो उपकरण (ल्यापटप, मोबाइल आदि) मार्फत् सामाजिक सञ्जाल प्रयोग गर्दा होसियार रहनुहोस् ।
- सामाजिक सञ्जालमा आफ्नो व्यक्तिगत सूचनाहरू सीमित रूपमा मात्र राख्नुहोस् ।
- आफ्नो व्यक्तिगत सूचना दुरुपयोगको जोखिम न्यूनीकरण गर्न आफूले चिनेका व्यक्तिहरूलाई मात्र सामाजिक सञ्जालमा साथी बनाउनुहोस् ।
- आफ्नो पोष्टहरूमा स्थान त्याग गर्दा होस् पुर्याउनुहोस् ।
- कुनै फोटो वा भिडियो अपलोड गर्दै हुनुहुन्छ भने उक्त फोटो र भिडियोमा भएका व्यक्तिहरूको अनुमति लिन नबिर्सिनुहोस् ।

- सुरक्षित मेसेजिङका लागि सिग्नल (Signal) एपको प्रयोग गर्नुहोस् ।
- सामाजिक सञ्जालमा पासवर्डहरू नियमित (कम्तीमा ३ महिनामा एकपटक) परिवर्तन गर्नुहोस् ।
- सामाजिक सञ्जालका मेसेजिङ एप (जस्तैः Messenger) आदिमार्फत संवेदनशिल सूचनाहरू आदानप्रदान नगर्नुहोस्।

अभियानकर्ताहरूका लागि डिजिटल सुरक्षाका केही सुझावहरू

- आफ्नो फोन र ल्यापटप दुवैमा पासवर्ड हालेर सुरक्षित बनाउनु होस् ।
- फोन र ल्यापटप दुवैमा भरपर्दो एन्टिभाइरस (Antivirus) इन्सटल गर्नुहोस् ।
- ब्राउजरमा (Browser) https:// राखेर मात्र ब्राउजिङ गर्नुहोस् ।
- भिडियोद्वारा गरिनु पर्ने बैठकको लागि जुम (Zoom), जित्सी (Jitsi) जस्ता प्लेटफर्मको प्रयोग गर्न सक्नु हुन्छ ।
- व्यक्तिगत सुरक्षा आदानप्रदानका लागि end to end encrypted मेसेजिङ एप्सहरू जस्तैः सिग्नल (Signal), टेलिग्राम (Telegram) आदिको प्रयोग गर्न सक्नु हुन्छ ।
- संवेदनशील डाटा आदानप्रदानका लागि प्रोटोनमेल (Proton mail), टुटानोटा (Tutanota) जस्ता इन्क्रिप्सन (Encryption) भएका इमेल प्लेटफर्महरूको प्रयोग गर्न सक्नु हुन्छ ।