प्रयोगात्मक हाते पुस्तिका

डिजिटल अधिकार तथा सुरक्षा, सूचना अखण्डता र निर्वाचन रिपोर्टिङ

Digital Rights Nepal

नेपाल पत्रकार महासंघ

डिजिटल अधिकार तथा सुरक्षा, सूचना अखण्डता र निर्वाचन रिपोर्टिङ

प्रयोगात्मक हाते पुस्तिका

Digital Rights Nepal

डिजिटल राइट्स नेपाल

नेपाल पत्रकार महासंघ

लेखन तथा सम्पादन
अधिवक्ता सन्तोष सिग्देल

लेखन सहयोगी
अधिवक्ता सन्जिना क्षेत्री
अधिवक्ता सदिच्छा सिलवाल
सौरभ भट्टराई

समीक्षा
निर्मला शर्मा
रामप्रसाद दाहाल
उज्ज्वल आचार्य
सरोज लामिछाने

प्रकाशन सहयोग
मिडिया डिफेन्स

प्रकाशक
डिजिटल राइट्स नेपाल
पुस २०८२

प्राक्कथन

डिजिटल युगमा पत्रकारिता अभ्याससँग जोडिएका अवसर, चुनौती र जोखिमहरूलाई सम्बोधन गर्ने उद्देश्यसहित *डिजिटल अधिकार तथा सुरक्षा, सूचना अखण्डता र निर्वाचन रिपोर्टिङ (प्रयोगात्मक हाते पुस्तिका)* तयार गरिएको हो। इन्टरनेट, सामाजिक सञ्जाल र आर्टिफिसियल इन्टेलिजेन्सको तीव्र विकासले समाचार सङ्कलन, सम्पादन र वितरणको स्वरूप परिवर्तन गरिरहेको वर्तमान सन्दर्भमा पत्रकारहरूको डिजिटल सुरक्षा, अधिकार संरक्षण र व्यावसायिक उत्तरदायित्वबारे स्पष्ट मार्गदर्शनको आवश्यकता बढेको छ। यही आवश्यकता महसुस गर्दै नेपाल पत्रकार महासंघसँगको सहकार्यमा डिजिटल राइट्स नेपालले यो हाते पुस्तिका तयार गरेको हो।

यो हाते पुस्तिका तयार गर्ने क्रममा निरन्तर सहकार्य, मार्गदर्शन तथा संस्थागत सहयोग प्रदान गर्नुहुने नेपाल पत्रकार महासंघप्रति हार्दिक आभार व्यक्त गर्दछु। यस दस्तावेजको विकासका क्रममा भएका परामर्श बैठकहरूबाट प्राप्त सुझाव र प्रतिक्रियाले हाते पुस्तिकालाई यथार्थपरक र उपयोगी बनाउन महत्त्वपूर्ण योगदान पुऱ्याएको छ। यस प्रक्रियामा नेतृत्वदायी भूमिका निर्वाह गर्नुहुने र हाते पुस्तिकाको मस्यौदा अध्ययन गरी महत्त्वपूर्ण सुझावहरू उपलब्ध गराउनुहुने अध्यक्ष निर्मला शर्मा तथा महासचिव रामप्रसाद दाहालप्रति विशेष धन्यवाद व्यक्त गर्दछु।

हाते पुस्तिकाको मूल सामग्री तयार गर्ने काममा संलग्न लेखन तथा सम्पादन समूहलाई हार्दिक धन्यवाद व्यक्त गर्दछु । डिजिटल अधिकार, डिजिटल सुरक्षा, तथ्यजाँच तथा निर्वाचन रिपोर्टिङका विषयमा उहाँहरूले गर्नुभएको अनुसन्धान र विश्लेषणले हाते पुस्तिकालाई उपयोगी र समयसापेक्ष बनाएको छ । यसैगरी, हाते पुस्तिकालाई अझ प्रयोगात्मक र उपयोगी तुल्याउन मस्यौदा अध्ययन गरी महत्त्वपूर्ण सुझावहरू उपलब्ध गराउनुहुने साइवर सुरक्षा विशेषज्ञ सरोज लामिछाने र सेन्टर फर मिडिया रिसर्चका निर्देशक उज्ज्वल आचार्यप्रति विशेष धन्यवाद ज्ञापन गर्दछु । उहाँहरूको सूक्ष्म समीक्षा र व्यवहारिक सुझावले पुस्तिकालाई यो स्वरूप दिन महत्त्वपूर्ण भूमिका खेलेको छ । यस पुस्तिकाको तयारी प्रक्रियाको व्यवस्थापकीय संयोजन गर्नुहुने डिजिटल राइट्स नेपालका दिलबहादुर कार्कीलाई धन्यवाद दिन चाहन्छु । त्यसै गरी यस पुस्तिकाको तयारी तथा प्रकाशनमा सघाउने मिडिया डिफेन्सप्रति पनि हार्दिक आभार प्रकट गर्दछु ।

यस पुस्तिकाले पत्रकारहरूलाई निर्वाचनका सन्दर्भमा सुरक्षित, जिम्मेवार र तथ्यपरक रिपोर्टिङ गर्नमा सहयोग पुर्‍याउनेछ साथै डिजिटल अधिकार, अभिव्यक्ति स्वतन्त्रता र पत्रकार सुरक्षा सम्बन्धी बहसलाई थप मजबुत बनाउँदै पत्रकारिता अभ्यासलाई थप सुरक्षित र उत्तरदायी बनाउने अपेक्षा गरेको छु ।

अधिवक्ता भोलानाथ ढुङ्गाना
अध्यक्ष
डिजिटल राइट्स नेपाल

आभार

डिजिटल युगमा पत्रकारिताको अभ्याससँग जोडिएका केही चुनौतीहरू र त्यसमा पनि विशेष गरी निर्वाचनको समयमा हुने जोखिम र जिम्मेवारीलाई सम्बोधन गर्ने उद्देश्यले डिजिटल अधिकार तथा सुरक्षा, सूचना अखण्डता र निर्वाचन रिपोर्टिङ (प्रयोगात्मक हाते पुस्तिका) नेपाल पत्रकार महासंघ र डिजिटल राइट्स नेपालसँगको सहकार्यमा तयार गरिएको हो। निर्वाचन रिपोर्टिङको क्रममा तथ्यपरकता, सन्तुलन, डिजिटल सुरक्षा र पत्रकारको अधिकार संरक्षण अत्यन्त महत्वपूर्ण हुन्छ; त्यसैले यस प्रकारको व्यवहारिक सामग्री समयसापेक्ष र आवश्यक छ।

यस हाते पुस्तिकाको तयारीमा नेतृत्वदायी भूमिका निर्वाह गर्नुहुने डिजिटल राइट्स नेपालका अध्यक्ष भोला नाथ ढुङ्गाना र कार्यकारी निर्देशक सन्तोष सिग्देल, सामग्री तयार गर्न संलग्न सम्पूर्ण लेखकहरू तथा समीक्षात्मक योगदान पुर्‍याउने समीक्षक टोलीप्रति नेपाल पत्रकार महासंघको तर्फबाट हार्दिक धन्यवाद व्यक्त गर्दछु। उहाँहरूको ज्ञान, अनुभव र व्यावसायिक प्रतिबद्धताले निर्वाचनको सन्दर्भमा पत्रकारहरूका लागि उपयोगी मार्गदर्शन उपलब्ध गराएको छ।

हाते पुस्तिकाले निर्वाचन अवधिमा डिजिटल माध्यम प्रयोग गरेर रिपोर्टिङ गर्दा अपनाउनु पर्ने सावधानी, आचारसंहिताको पालना र जोखिम न्यूनीकरणमा पत्रकारहरूलाई महत्वपूर्ण सहयोग पुर्‍याउने छ।

निर्मला शर्मा
अध्यक्ष
नेपाल पत्रकार महासंघ

शुभकामना

प.सं. च.नं. / Ref:

प्रतिनिधि सभा सदस्य निर्वाचन, २०८२ को पूर्वसन्ध्यामा नेपाल पत्रकार महासंघ र डिजिडल राइट्स नेपालको सहकार्यमा **"डिजिटल अधिकार तथा सुरक्षा, सूचना अखण्डता र निर्वाचन रिपोर्टिङ्ग"** सम्बन्धी प्रयोगात्मक हातेपुस्तिका प्रकाशन हुन लागेकोमा अत्यन्त खुशी लागेको छ। सूचना प्रविधिको चरम विकास भएको वर्तमान समयमा निर्वाचन सम्बन्धी समाचार संकलन, सम्पादन तथा सम्प्रेषणमा सूचना सदाचार प्रवर्द्धन गरी आमनागरिकलाई यथार्थ सूचना प्रवाह गर्ने ध्येयले तयार गरिएको यस समयसापेक्ष र सान्दर्भिक प्रकाशनका लागि दुवै संस्थालाई हार्दिक बधाई दिंदै प्रकाशनको सफलताको शुभकामना व्यक्त गर्दछु। यस हातेपुस्तिकाले सञ्चारकर्मी तथा सञ्चार संस्थाहरूलाई निर्वाचन सम्बन्धी डिजिटल जोखिम पहिचान गर्न, गलत तथा भ्रामक सूचनासँग जुध्न एवम् सुरक्षित तथा जिम्मेवार रिपोर्टिङ्ग अभ्यास गर्न व्यवहारिक मार्गदर्शन गर्नुका साथै निर्वाचनसँग सम्बन्धित दुष्प्रचार, मिथ्या सूचना र द्वेषपूर्ण अभिव्यक्तिलाई निस्तेज गरी मतदातालाई निर्वाचन सम्बन्धी सही सूचना र जानकारी प्राप्त गर्नमा समेत सहयोगी सिद्ध हुनेछ भन्ने विश्वास लिएको छु।

निर्वाचन आयोग स्वच्छ, स्वतन्त्र, निष्पक्ष, समावेशी र शान्तिपूर्ण निर्वाचन सम्पन्न गराउन सदैव प्रतिवद्ध रहेको छ। आयोगले सञ्चार जगत लगायत सबै सरोकारवालासँगको सहकार्यमा निर्वाचन सञ्चालन तथा व्यवस्थापनका पद्धति र प्रविधिमा समयानुकूल सुधार गर्दै सूचना प्रविधिको उपयोग एवम् हरित निर्वाचनमा समेत जोड दिएको छ। यसका लागि आयोगमा निर्वाचन सूचना संप्रेषण तथा समन्वय केन्द्रको स्थापना गरी उक्त केन्द्र अन्तर्गत डिजिटल मतदाता शिक्षा इकाइ, प्रेस अफिस र सूचना सदाचार प्रवर्द्धन इकाइ समेत सञ्चालन गरिएको छ भने निर्वाचन आचारसंहितामा निर्वाचनको प्रचारप्रसार गर्दा डिजिटल प्रचारप्रसारलाई प्राथमिकता दिनुपर्ने व्यवस्था गरिएको छ। यसरी निर्वाचन प्रक्रियामा सूचना प्रविधिको प्रयोग विस्तारसँगै डिजिटल अधिकारको संरक्षण, डिजिटल सुरक्षा, सूचनाको अखण्डता र जिम्मेवार निर्वाचन रिपोर्टिङ्गको महत्व बढेर गएको छ। यी विषयहरूलाई व्यवहारिक उपयोगमा ल्याउने प्रयासहरू आवश्यक देखिएको सन्दर्भमा यस हातेपुस्तिकाले निर्वाचन आचारसंहिताको पालना, तथ्यमा आधारित निर्वाचनसम्बन्धी सूचना संप्रेषण तथा डिजिटल सुरक्षा मार्फत स्वतन्त्र, निष्पक्ष र सुरक्षित निर्वाचन वातावरण निर्माणमा योगदान पुऱ्याउने विश्वास लिएको छु।

अन्त्यमा, यस महत्वपूर्ण र समयसापेक्ष प्रकाशनका लागि नेपाल पत्रकार महासंघ र डिजिटल राइट्स नेपाललाई धन्यवाद दिंदै आगामी दिनमा समेत यस्तै रचनात्मक क्रियाशीलता मार्फत निर्वाचन र लोकतन्त्रको सुदृढीकरणमा निरन्तर योगदानका लागि शुभकामना व्यक्त गर्दछु। धन्यवाद।

राम प्रसाद भण्डारी
कार्यवाहक प्रमुख निर्वाचन आयुक्त

"स्वतन्त्र र निष्पक्ष निर्वाचन: राष्ट्रको गौरव"
"Free and Fair Election: Pride of Nation"
कान्तिपथ, काठमाडौं, नेपाल, फोन नं.: (९७७-१) ५३२८६६३ । फ्याक्स: (९७७-१) ५३२५५८०
Kantipath, Kathmandu, Nepal, Tel: (977-1) 5328663, Fax: (977-1) 5325580
E-mail: info@election.gov.np, Website: www.election.gov.np

विषयसूची

परिचय

पृष्ठभूमि

इन्टरनेटको बढ्दो प्रयोग र त्यसले समाजमा पारिरहेको प्रभाव आज सर्वत्र छलफलको विषय बनेको छ । पछिल्ला वर्षहरूमा आर्टिफिसियल इन्टेलिजेन्स (ए.आई.) को तीव्र विकास र प्रयोगसँगै इन्टरनेट र एआई दुवै हरेक बहस, गोष्ठी र नीतिगत छलफलको महत्त्वपूर्ण पाटो बनेका छन् । पत्रकारिता क्षेत्रलाई हेर्ने हो भने समाचार सङ्कलन, सम्पादन र वितरणको प्रक्रियामा प्रविधिले आमूल परिवर्तन ल्याएको छ भने पत्रकारिता अब केवल फिल्ड रिपोर्टिङमा सीमित नरही मोबाइल फोन, सामाजिक सञ्जाल र अनलाइन प्लेटफर्ममार्फत पत्रकारहरू चौबीसै घण्टा सूचनाको प्रवाहमा संलग्न छन् । यसले एकातिर सूचनाको पहुँच र प्रभाव बढाएको छ भने अर्कोतर्फ पत्रकारका लागि नयाँ जिम्मेवारी, जोखिम र दबाव पनि थपेको छ ।

नेपालको सन्दर्भमा पछिल्ला केही वर्षदेखि देखिएको राजनीतिक ध्रुवीकरण, सडक आन्दोलन, Gen Z आन्दोलन, तथा विभिन्न प्रकारका विरोध प्रदर्शनहरू लगायतका घटनाहरूले मिडिया र पत्रकारको भूमिकालाई एकदम संवेदनशील र चुनौतीपूर्ण बनाएको छ । यस्ता घटनाहरूको रिपोर्टिङ गर्ने क्रममा पत्रकारहरूले शारीरिक जोखिम मात्र होइन, समाचार प्रकाशन वा प्रसारणपछि अनलाइन आक्रमण, घृणात्मक टिप्पणी, ट्रोलिङ, चरित्र हत्या र लक्षित दुष्प्रचारको सामना गर्नुपरेको छ । कतिपय अवस्थामा अभिव्यक्ति स्वतन्त्रता, गोपनीयता र सूचनामा पहुँच लगायतका डिजिटल अधिकारहरू सीधै प्रभावित भएका उदाहरणहरू पनि देखिएका छन् ।

तस्बिरमा छेडछाड गरी परिवर्तन गर्ने, भिडियोका दृश्यहरूलाई सन्दर्भबाट अलग गरी काँटछाँट गर्ने वा केही अंश मात्र चयन गरेर वा सम्पादन गरी मिथ्या वा भ्रामक सूचनासहित पुनः प्रसार गर्ने, व्यक्तिगत सामाजिक सञ्जाल पोस्टलाई आधार बनाएर समाचार संस्थामाथि आक्रमण गर्ने, वा संवेदनशील रिपोर्टिङको कारण साइवर अपराध, गाली बेइज्जती वा अदालतको अपहेलनमा मुद्दा चलाउने जस्ता घटनाहरू पछिल्ला वर्षहरूमा बारम्बार देखिएका छन्। यस्ता घटनाहरुले डिजिटल स्पेसमा पत्रकारको सुरक्षा कमजोर र चुनौतीपूर्ण बन्दै गएको छ भन्ने यथार्थ उजागर गर्छन्।

विगतका अनुभवहरूलाई हेर्ने हो निर्वाचन अवधिमा माथि उल्लिखित चुनौती र जोखिमहरू अझै तीव्र हुन्छन्। २०७४ र २०७९ का निर्वाचनका समयमा सामाजिक सञ्जालमार्फत उम्मेदवारका कथित अडियो-भिडियो, पुराना तस्बिरहरू वा सन्दर्भविहीन अभिव्यक्तिहरू काँटछाँट गरी भाइरल बनाइएका घटनाहरू देखिएका थिए। उम्मेदवार, राजनीतिक दल र समर्थकहरूबीचको तीव्र प्रतिस्पर्धा समाचार सामग्रीमा पनि प्रतिबिम्बित हुन्छ, जहाँ सानो त्रुटि, अपुरो सन्दर्भ वा भ्रामक प्रस्तुतीकरणले ठूलो राजनीतिक र सामाजिक प्रभाव पार्न सक्छ। यही अनुभवका आधारमा पनि निर्वाचनका अवधिमा पत्रकारले तथ्यमा आधारित, सन्तुलित र निष्पक्ष रिपोर्टिङ गर्नु मात्र होइन, आफ्नै डिजिटल सुरक्षा र अधिकारको संरक्षणप्रति पनि सचेत रहनु कति महत्त्वपूर्ण छ भन्ने देखाएको छ ।

हाते पुस्तिकाको उद्देश्य

नेपाल पत्रकार महासंघसँगको सहकार्यमा डिजिटल राइट्स नेपालले तयार गरेको यस हाते पुस्तिकाको मुख्य उद्देश्य पत्रकारहरूलाई सुरक्षित, जिम्मेवार र तथ्यपरक रूपमा निर्वाचन तथा संवेदनशील घटनाहरूको रिपोर्टिङमा सहयोग पुर्‍याउनु हो। यस हाते पुस्तिकामा प्रेस काउन्सिल नेपालले जारी गरेको पत्रकार आचारसंहिता, २०७३ (पहिलो संशोधन २०७६) र निर्वाचन आयोगद्वारा प्रकाशित निर्वाचन आचारसंहिता, २०८२ का डिजिटल सञ्चार माध्यममा लागू हुने प्रावधानहरूलाई

सन्दर्भमा लिई निर्वाचनको समयमा पत्रकारहरूले डिजिटल माध्यममा आचारसंहिताको पालना गर्दै रिपोर्टिङ गर्न सक्ने दिशानिर्देशहरू प्रस्तुत गरिएको छ।

यस हाते पुस्तिका तयार गर्नुका प्रमुख उद्देश्यहरू यस प्रकार छन्:

- डिजिटल युगमा पत्रकारहरूले सामना गरिरहेका नयाँ चुनौती र जोखिमबारे सचेत गराउने।
- निर्वाचन प्रक्रिया, डिजिटल मिडिया र डिजिटल अधिकारबीचको सम्बन्धबारेको बुझाइलाई थप स्पष्ट बनाउने।
- डिजिटल सुरक्षा, गोपनीयता र जोखिम न्यूनीकरणका व्यावहारिक उपाय र सीप प्रदान गर्ने।
- नयाँ डिजिटल प्रविधि, सामाजिक सञ्जाल र अनलाइन उपकरणहरूको प्रयोग गरी निर्वाचन तथा अन्य संवेदनशील विषयमा रिपोर्टिङ गर्दा पत्रकारले अपनाउनुपर्ने जिम्मेवार, सुरक्षित र नैतिक अभ्यासहरूमा प्रकाश पार्ने।
- आगामी निर्वाचन तथा संवेदनशील राजनीतिक–सामाजिक घटनाहरूमा पत्रकारहरूलाई सुरक्षित, जिम्मेवार र व्यावसायिक रिपोर्टिङ गर्न सक्षम बनाउने।

हाते पुस्तिकाको दायरा र सीमा

यो हाते पुस्तिका मुख्यतः डिजिटल स्पेसमा कार्यरत पत्रकारितालाई लक्षित गरी तयार गरिएको हो। त्यसैले यसमा समेटिएका अधिकांश विश्लेषण, जोखिम मूल्याङ्कन, उदाहरण र सिफारिसहरू अनलाइन पत्रकारिता, सामाजिक सञ्जाल, डिजिटल प्लेटफर्म, मोबाइल जर्नालिज्म तथा इन्टरनेटमा आधारित समाचार उत्पादन र वितरण प्रक्रियासँग प्रत्यक्ष रूपमा सम्बन्धित छन्। छापा माध्यम,

टेलिभिजन, रेडियो जस्ता परम्परागत माध्यममा लागू हुने सबै पक्षहरूलाई यस हाते पुस्तिकाले विस्तृत रूपमा समेट्ने उद्देश्य राखेको छैन ।

तर, यस हाते पुस्तिकामा समावेश गरिएको डिजिटल सुरक्षा, गोपनीयता संरक्षण, मिथ्या सूचना पहिचान, अनलाइन आक्रमणबाट जोगिने उपाय र जोखिम न्यूनीकरणका सीपहरू भने डिजिटल पत्रकारितामा मात्र सीमित छैनन् । यी विषयवस्तुहरू छापा, रेडियो वा टेलिभिजनजस्ता अन्य माध्यममा कार्यरत पत्रकारहरूका लागि पनि उपयोगी र सान्दर्भिक हुन सक्छन् ।

त्यसैगरी, हाते पुस्तिकाको एक महत्त्वपूर्ण परिच्छेद निर्वाचन रिपोर्टिङमा केन्द्रित छ । यस परिच्छेदमा निर्वाचनसँग सम्बन्धित डिजिटल अभियानहरुका सामग्रीमा सम्भावित हेरफेर पहिचान गर्ने तरिका, भाइरल अफवाह र मिथ्या सूचना उपरको द्रुत प्रतिक्रियाका उपायहरु, डिजिटल रिपोर्टिङमा मतदाता र स्रोतको गोपनीयता सुनिश्चित गर्ने तरिकाहरु जस्ता विषयहरूलाई छलफल गरिएको छ ।

यस हाते पुस्तिकालाई सम्पूर्ण पत्रकारिता अभ्यासको पूर्ण मार्गदर्शक भन्दा पनि डिजिटल युगमा, विशेषगरी निर्वाचन र संवेदनशील राजनीतिक तथा सामाजिक सन्दर्भमा पत्रकारहरूलाई सुरक्षित, सचेत र जिम्मेवार रिपोर्टिङतर्फ उन्मुख गराउने व्यावहारिक सन्दर्भ सामग्रीका रूपमा बुझ्न सकिन्छ ।

परिच्छेद १

डिजिटल अधिकार र जिम्मेवारीहरु

१. डिजिटल अधिकारको परिचय

१.१ पत्रकारहरूका लागि डिजिटल अधिकारको अर्थ र महत्त्व

नेपालमा पछिल्ला वर्षहरूमा पत्रकारिताको माध्यम र अभ्यासका साथसाथै समाचार उपभोगको माध्यममा समेत उल्लेखनीय परिवर्तन आएको छ। इन्टरनेट, सामाजिक सञ्जाल र नयाँ डिजिटल प्रविधिले समाचार सङ्कलन, उत्पादन, प्रसारण र उपभोगको तरिकालाई व्यापक रूपमा बदलिदिएको छ। आज इन्टरनेट सूचना पहुँचको सबैभन्दा प्रमुख माध्यम बनेको छ, जहाँ समाचारका प्राथमिक स्रोतहरू परम्परागत मिडियासँगै फेसबुक, एक्स (ट्विटर), टिकटक र युट्युबजस्ता डिजिटल प्लेटफर्महरूमा केन्द्रित हुँदै गएका छन्। यस्तो डिजिटल वातावरणमा पत्रकारहरूले आफ्ना डिजिटल अधिकार जस्तै अभिव्यक्ति स्वतन्त्रता, गोपनीयता, व्यक्तिगत डाटाको सुरक्षा, अनलाइन सुरक्षा र डिजिटल पहुँच बारे स्पष्ट बुझाइ राख्नु अत्यन्त आवश्यक छ।

आजका नेपाली पत्रकारहरू समाचार कक्षमा मात्र सीमित छैनन्। मोबाइल फोन, क्यामेरा र सामाजिक सञ्जाल धेरै पत्रकारका लागि पेसागत कामका प्रमुख उपकरण बनेका छन्। नागरिकसँग प्रत्यक्ष सम्पर्क, सूचना सङ्कलन र समाचार वितरण प्रायः अनलाइन प्लेटफर्ममार्फत हुने गरेको छ। तर यही डिजिटल स्पेस पत्रकारका लागि अवसरसँगै जोखिमको क्षेत्र पनि बनेको छ। पत्रकार र मिडियाविरूद्धको सामाजिक

सञ्जालमार्फत हुने लक्षित आक्रमण, संयोजित बदनामी अभियान, ट्रोलिङ बढ्दै गएको देखिन्छ भने कानुनलाई नै हतियारका रूपमा प्रयोग गरी साइवर अपराध, गाली बेइज्जतीका मुद्दा चलाइएका घटनाहरू समेत बढेका छन् । निर्वाचन जस्तो संवेदनशील वातावरणमा पत्रकारका हरेक शब्द, पोस्ट वा भिडियो स्क्रिनसट भएर सन्दर्भविहीन रूपमा प्रयोग हुन सक्ने सम्भावना रहन्छ, जसले पत्रकारलाई कानुनी, सामाजिक वा व्यक्तिगत जोखिममा पार्न सक्छ ।

नेपालमा जारी राजनीतिक उतारचढाव, आन्दोलन र विरोध प्रदर्शनको बीचमा पत्रकारको भूमिका एकदम संवेदनशील र महत्त्वपूर्ण बन्दै गएको छ । यस्तो अवस्थामा तथ्यपूर्ण र सन्तुलित सूचना सार्वजनिक गर्नु पत्रकारको पेसागत दायित्व हो । तर, यिनै गतिविधि समेट्ने क्रममा पत्रकारहरूले शारीरिक आक्रमण, दुर्व्यवहार, काममा हस्तक्षेप, धम्की र उपकरण तोडफोडजस्ता जोखिम सामना गर्नुपरेको छ । २०८१ चैत्र १५ गतेको घटनामा पत्रकार सुरेश रजकको मृत्यु तथा Gen Z आन्दोलनका क्रममा मिडिया हाउस र पत्रकारमाथि भएको आक्रमण जस्ता घटनाले आन्दोलन र राजनीतिक तनावको समयमा मिडिया र पत्रकार कतिसम्म असुरक्षित हुन सक्छन् भन्ने स्पष्ट देखाएका छन् ।

यस्ता जोखिमहरू सबै पत्रकारका लागि एकै स्वरूपका वा एकै जोखिमका भने छैनन् । महिलाहरू, दलित तथा लैङ्गिक अल्पसङ्ख्यक समुदायका पत्रकारहरूले दोहोरो जोखिम सामना गरिरहेका छन् । रिपोर्टिङकै कारण मात्र होइन, आफ्नै पहिचानका कारण पनि उनीहरू लक्षित गालीगलौज, चरित्र हत्या, यौनिक वा घृणात्मक टिप्पणी, धम्की र डरत्रासको सिकार बन्ने गरेका छन् । कतिपय अवस्थामा समाचारको बाइ-लाइनमा नाम प्रकाशित हुनु नै जोखिमको कारण बन्ने गरेको छ । यसले पत्रकारको पेसागत स्वतन्त्रता, मानसिक स्वास्थ्य र सुरक्षित रूपमा काम गर्ने अधिकारमाथि गम्भीर प्रश्न उठाएको छ ।

यस सन्दर्भमा पत्रकारका लागि डिजिटल अधिकार भनेको केवल प्रविधिको प्रयोगसँग सम्बन्धित विषय मात्र होइन । यो सुरक्षित पत्रकारिता, प्रेस स्वतन्त्रता, आत्मसम्मान, र लोकतान्त्रिक प्रक्रियाको आधारभूत सर्त हो । डिजिटल अधिकारको

संरक्षण बिना न त स्वतन्त्र पत्रकारिता सम्भव हुन्छ, न त नागरिकको सूचनामा पहुँच सुनिश्चित गर्न सकिन्छ । त्यसैले डिजिटल अधिकारको स्पष्ट बुझाइ र संरक्षण पत्रकारको पेसागत दायित्व र सुरक्षाको अभिन्न हिस्सा हो ।

१.२ डिजिटल अधिकारका मुख्य आयामहरू

डिजिटल अधिकार भन्नाले सामान्यतया इन्टरनेट र डिजिटल माध्यम प्रयोग गर्न, सूचनामा पहुँच पाउन, आफ्ना विचार स्वतन्त्र रूपमा अभिव्यक्त गर्न, तथा व्यक्तिगत गोपनीयता र डाटाको सुरक्षा सुनिश्चित गर्न पाउने अधिकारलाई जनाउँछ । डिजिटल अधिकार कुनै नयाँ वा अलग अधिकार होइनन्; यी अफलाइन जीवनमा सुनिश्चित गरिएका मौलिक अधिकारहरूको डिजिटल विस्तार हुन् । जसरी हामी भौतिक संसारमा अभिव्यक्ति स्वतन्त्रता, गोपनीयता र सूचनाको अधिकार प्रयोग गर्छौं, त्यस्तै अधिकारहरू इन्टरनेट र डिजिटल स्पेसमा पनि सुरक्षित रूपमा प्रयोग गर्न पाउनुपर्छ ।

संयुक्त राष्ट्र सङ्घले इन्टरनेटको पहुँचमा रोक लगाउनु डिजिटल अधिकारको उल्लङ्घन हो र यस्तो कार्य अन्तर्राष्ट्रिय कानुनको विरुद्ध हुन्छ भनेर स्पष्ट रुपमा उल्लेख गरेको छ ।[1] इन्टरनेटको बढ्दो प्रयोगसँगै डिजिटल अधिकारको महत्त्व पनि झन् बढ्दै गएको छ भने विशेषगरी पत्रकारिता जस्तो सार्वजनिक चासोको पेशामा यसको महत्त्व अझ ज्यादा छ ।

नेपालमा इन्टरनेट र सामाजिक सञ्जालको प्रयोग तीव्र रूपमा बढेसँगै गोपनीयता उल्लङ्घन, व्यक्तिगत डाटाको दुरुपयोग, मिथ्या सूचना र अभिव्यक्तिमाथि नियन्त्रणका घटनाहरू पनि बढिरहेका छन् । निर्वाचन जस्ता संवेदनशील समयमा डिजिटल प्लेटफर्ममार्फत सूचनाको तीव्र प्रवाह हुन्छ, त्यसैका आधारमा जनमत निर्माण तथा मिथ्या एवम् भ्रामक सूचनाले मतदाताको निर्णयमा प्रत्यक्ष प्रभाव पार्न सक्ने भएकाले यी चुनौतीहरू थप गम्भीर हुन्छन् । त्यसैले पत्रकारहरूका लागि डिजिटल अधिकारको बुझाइ र यसको जिम्मेवार प्रयोग अत्यन्त आवश्यक छ ।

1 https://docs.un.org/en/A/RES/78/213

यस परिच्छेदमा निर्वाचन तथा संवेदनशील रिपोर्टिङको सन्दर्भमा पत्रकारका लागि महत्त्वपूर्ण डिजिटल अधिकारका प्रमुख आयामहरूलाई निम्न शीर्षकहरू अन्तर्गत प्रस्तुत गरिएको छ।

१. अनलाइन अभिव्यक्ति स्वतन्त्रता

अभिव्यक्ति स्वतन्त्रता लोकतान्त्रिक समाजको आधारभूत स्तम्भ हो। स्वतन्त्र, निर्बाध र सेन्सरशीप-रहित प्रेसले नागरिकलाई सूचना प्राप्त गर्ने, विचार निर्माण गर्ने र सार्वजनिक बहसमा सहभागी हुने अवसर प्रदान गर्छ। यही कारणले अन्तर्राष्ट्रिय मानव अधिकार कानुनले अभिव्यक्ति स्वतन्त्रतालाई आधारभूत अधिकारका रूपमा मान्यता दिएको छ।[2]

इन्टरनेटमा अभिव्यक्ति स्वतन्त्रतासम्बन्धी केही प्रमुख सिद्धान्तहरू पत्रकारका लागि विशेष रूपमा महत्त्वपूर्ण छन्:

- अभिव्यक्ति स्वतन्त्रता सञ्चारका अन्य माध्यमहरूमा जस्तै इन्टरनेटमा पनि पूर्ण रूपमा लागू हुन्छ। इन्टरनेटमा अभिव्यक्तिमाथि प्रतिबन्ध लगाउनुपरेमा स्थापित अन्तर्राष्ट्रिय मानव अधिकार मापदण्डअनुसार, कानुनी रूपमा स्पष्ट र आवश्यक भएको अवस्थामा मात्र लगाइनुपर्छ।
- कुनै पनि प्रतिबन्ध आवश्यक, वैध र समानुपातिक हुनुपर्छ। यस्तो प्रतिबन्धले इन्टरनेटले प्रदान गर्ने सूचनाको पहुँच, बहस र विविध विचार अभिव्यक्त गर्ने क्षमतामा पर्ने असरलाई ध्यानमा राखेर मूल्याङ्कन गर्नुपर्छ।
- टेलिफोन वा प्रसारणजस्ता परम्परागत सञ्चार माध्यमका नियमहरू जस्ताको तस्तै इन्टरनेटमा लागू गर्नु उपयुक्त हुँदैन। इन्टरनेटको खुलापन, पहुँच र अन्तरक्रियात्मक प्रकृतिलाई ध्यानमा राखी विशेष नीति र कानुनी व्यवस्था आवश्यक हुन्छ।

2 https://www.ohchr.org/sites/default/files/english/bodies/hrc/docs/gc34.pdf

- गैरकानुनी सामग्री नियन्त्रणका नाममा सम्पूर्ण प्लेटफर्म वा अस्पष्ट "विशेष सामग्री" माथि व्यापक प्रतिबन्ध लगाइनु हुँदैन। बरु इन्टरनेटको विशेषतासँग अनुकूल वैकल्पिक र लक्षित उपायहरू अपनाइनुपर्छ।
- घृणायुक्त अभिव्यक्तिको सामना गर्न स्वनियमन (self-regulation) महत्त्वपूर्ण उपाय हो। पत्रकार, मिडिया संस्था र डिजिटल प्लेटफर्महरूले पेसागत आचारसंहिता र जिम्मेवार अभ्यासलाई प्राथमिकता दिनुपर्छ।
- डिजिटल स्पेसको जिम्मेवार प्रयोग प्रवर्द्धन गर्न सचेतना अभिवृद्धि, तालिम र मिडिया साक्षरतामा लगानी आवश्यक छ।

२. सूचनाको अधिकार

सूचनाको अधिकार डिजिटल अधिकारको केन्द्रीय आयाम हो । डिजिटल युगमा नागरिकले सूचनामा पहुँच कागजी अभिलेखमार्फत मात्र होइन, अनलाइन प्लेटफर्म, सरकारी वेबसाइट र डिजिटल डाटाबेसमार्फत पनि पाउनुपर्छ । त्यसैले सूचनाको अधिकार भनेको डिजिटल रूपमा सूचना खोज्न, प्राप्त गर्न र प्रयोग गर्न सक्ने अधिकारसमेत हो ।

पत्रकारका लागि सूचनाको अधिकार तथ्यमा आधारित पत्रकारिताको आधार हो । सरकारले सङ्कलन र प्रयोग गर्ने सूचनामा पहुँचबिना सार्वजनिक पदमा रहेका व्यक्तिलाई जवाफदेही बनाउन वा निर्वाचनसम्बन्धी विषयहरू जस्तै मतदाता सूची, उम्मेदवार, खर्च, प्रक्रिया, निर्वाचन नतिजा आदिका बारेमा विश्वसनीय रिपोर्टिङ गर्न सम्भव हुँदैन ।

यद्यपि, डिजिटल माध्यममार्फत सूचना सार्वजनिक गर्ने अभ्यास बढ्दै गए पनि व्यवहारमा सूचना नदिने, ढिलाइ गर्ने, अपुरो वा प्रयोग गर्न नसकिने ढाँचामा सूचना उपलब्ध गराउने समस्या कायमै छन् । वेबसाइट बन्द हुनु, डाटा हटाइनु वा "प्राविधिक कारण" देखाएर सूचना अवरुद्ध गरिनु पनि डिजिटल सूचनाको अधिकारमाथिको अप्रत्यक्ष प्रतिबन्ध हुन सक्छ । सूचनाको अधिकार अभिव्यक्ति स्वतन्त्रतासँग प्रत्यक्ष रूपमा जोडिएको छ । सूचना बिना अभिव्यक्ति कमजोर हुन्छ ।

पत्रकारले मिथ्या वा भ्रामक सूचनाको खण्डन गर्न, तथ्य प्रमाणित गर्न र सार्वजनिक बहसलाई सही दिशामा लैजान सूचनामा पहुँच अनिवार्य हुन्छ।

यस सन्दर्भमा पत्रकारको भूमिका सूचना प्राप्तिमा सीमित छैन। डिजिटल स्पेसमा सूचना कसरी उपलब्ध गराइँदैछ, कुन सूचना सार्वजनिक हितका बाबजुद लुकाइँदैछ, र सूचनाको अभावले कसलाई असर पारिरहेको छ भन्ने प्रश्न उठाउनु पनि पत्रकारको दायित्व हो। विशेषगरी निर्वाचनको समयमा आधिकारिक सूचनामा पहुँच र पारदर्शिता सुनिश्चित गर्नु डिजिटल अधिकार र लोकतन्त्र दुवैका लागि अपरिहार्य हुन्छ।

३. गोपनीयता र तथ्याङ्क संरक्षण

गोपनीयताको अधिकार राष्ट्रिय कानुनका साथै नागरिक तथा राजनीतिक अधिकारसम्बन्धी अन्तर्राष्ट्रिय प्रतिज्ञा पत्र (ICCPR, दफा १७) द्वारा सुरक्षित गरिएको छ। यस अनुसार कसैको निजी जीवन, परिवार, घर, पत्राचार वा प्रतिष्ठामा स्वेच्छाचारी वा गैरकानुनी हस्तक्षेप गर्न पाइँदैन, र यस्ता हस्तक्षेपविरुद्ध कानुनी संरक्षण पाउने अधिकार प्रत्येक व्यक्तिलाई छ।

राज्यको दायित्व भनेको नागरिकको निजी जीवनमा अनावश्यक हस्तक्षेप हुन नदिनु र गोपनीयताको प्रभावकारी संरक्षण गर्नु हो। गोपनीयताको अधिकार निजी मात्र होइन, सार्वजनिक क्षेत्रमा पनि लागू हुन्छ। यद्यपि राजनीतिज्ञ र सार्वजनिक पदधारी व्यक्तिहरूको हकमा सार्वजनिक चासोका कारण गोपनीयताको दायरा केही फराकिलो हुन सक्छ। तर पत्रकारहरूले यस्तो रिपोर्टिङ गर्दा पनि मानवीय मर्यादा, तथ्यमा आधारित र सार्वजनिक हितको मापदण्डलाई अनिवार्य रूपमा ध्यानमा राख्नुपर्छ। आधारविहीन आरोप, चरित्र हत्या वा प्रतिष्ठामा आँच पुर्‍याउने सामग्री प्रकाशन हुनु हुँदैन।

डिजिटल युगमा गोपनीयतासँगै तथ्याङ्क (डाटा) संरक्षणको महत्त्व अझ बढेको छ। मतदाता दर्तादेखि नतिजा प्रकाशनसम्मको सम्पूर्ण निर्वाचन प्रक्रिया नै

तथ्याङ्कमा आधारित हुन्छ । राजनीतिक दल र उम्मेदवारहरूले पनि अभियान सञ्चालन गर्दा मतदाताको डाटा प्रयोग गर्ने गर्छन् । माइक्रो-टार्गेटिङमार्फत मतदाता केन्द्रित सन्देश प्रवाह गर्ने अभ्यास बढ्दै गएको छ, जसमा डाटाको दुरुपयोग हुने जोखिम उच्च हुन्छ ।

मतदाताको व्यक्तिगत डाटा अवैध रूपमा सङ्कलन, विश्लेषण वा हेरफेर गरिएमा निर्वाचन प्रक्रियामाथि जनविश्वास कमजोर हुन सक्छ । त्यसैले राजनीतिक अभियान, मिडिया र सरोकारवाला सबैले डाटा सुरक्षाका स्थापित मुख्य सिद्धान्तहरू वैधता, आवश्यकता, पारदर्शिता र सुरक्षा अनुसार तथ्याङ्क प्रशोधन गर्नुपर्छ ।

पत्रकारका लागि गोपनीयता र डाटा संरक्षणको बुझाई दुई तहमा महत्त्वपूर्ण छ: पहिलो, आफू र आफ्ना स्रोतहरूको सुरक्षा सुनिश्चित गर्न; दोस्रो, निर्वाचन र डिजिटल अभियानमा हुने डाटा दुरुपयोगलाई पहिचान गरी सार्वजनिक चासोका विषयका रूपमा उजागर गर्न । यही जिम्मेवार अभ्यासले डिजिटल युगमा लोकतन्त्र र पत्रकारितामाथिको विश्वास मजबुत बनाउन सहयोग पुर्‍याउँछ ।

४. अनलाइन उत्पीडनबाट संरक्षण तथा डिजिटल सुरक्षा सुनिश्चितता

अनलाइन उत्पीडनबाट संरक्षण तथा डिजिटल सुरक्षा सुनिश्चितता पत्रकारका लागि डिजिटल अधिकारको अर्को अत्यन्त महत्त्वपूर्ण आयाम हो । डिजिटल वातावरणमा सक्रिय पत्रकारहरू ह्याकिङ, फिशिङ, खातामा पहुँच गर्न रोक्ने, डिभाइसमा अनधिकृत पहुँच, डाटा चोरी, तथा लक्षित साइबर आक्रमणको जोखिममा रहन्छन् । यस्ता आक्रमणहरूले व्यक्तिगत क्षति मात्र पुर्‍याउने नभई स्रोतको गोपनीयता, समाचार सामग्रीको विश्वसनीयता र सम्पूर्ण पत्रकारिता प्रक्रियामाथि नै गम्भीर असर पार्न सक्छन् । विशेषगरी निर्वाचन, आन्दोलन तथा राजनीतिक रूपमा संवेदनशील विषयमा रिपोर्टिङ गर्ने क्रममा हुने डिजिटल असुरक्षाले पत्रकारलाई निगरानी, धम्की र स्वनियन्त्रणतर्फ धकेल्ने सम्भावना रहन्छ । त्यसैले सुरक्षित पासवर्ड अभ्यास, दुई तहको प्रमाणीकरण, सुरक्षित सञ्चार माध्यमको प्रयोग, डिभाइस र डाटाको

नियमित सुरक्षा, तथा साइबर आक्रमणको जोखिम पहिचान र उक्त जोखिमहरूको सम्बोधन गर्ने उपायहरू अपनाउनु केवल प्राविधिक सावधानी मात्र नभई सुरक्षित, स्वतन्त्र र जिम्मेवार पत्रकारिताको आधारभूत सर्त हो। डिजिटल सुरक्षा सुनिश्चित नभएमा पत्रकारको पेसागत स्वतन्त्रतामा मात्र नभई नागरिकको विश्वसनीय सूचनाको अधिकारमा समेत प्रभाव पर्दछ।

१.३ दैनिक रिपोर्टिङमा डिजिटल अधिकार सुनिश्चित गर्ने पत्रकारको दायित्व

डिजिटल प्रविधिले पत्रकारिताको पहुँच, गति र प्रभाव अभूतपूर्व रूपमा बढाएको छ । तर यही प्रविधिका कारण पत्रकारिताले नयाँ जोखिम, नैतिक द्वन्द्व र अधिकारसम्बन्धी चुनौतीहरूको सामना समेत गर्नु परेको छ । डिजिटल युगमा पत्रकार केवल सूचनाका सङ्कलक र प्रसारक मात्र होइनन्; उनीहरू डिजिटल अधिकारका प्रयोगकर्ता, संरक्षक र प्रवर्द्धकसमेत हुन् । अभिव्यक्ति स्वतन्त्रता, सूचनाको अधिकार, गोपनीयता र तथ्याङ्क संरक्षणजस्ता डिजिटल अधिकारहरू पत्रकारको दैनिक कामसँग प्रत्यक्ष रूपमा जोडिएका छन्।

दैनिक रिपोर्टिङमा डिजिटल अधिकारको सम्मान नगर्दा त्यसको असर केवल सम्बन्धित व्यक्तिमा सीमित रहँदैन। मिथ्या वा भ्रामक सूचना, गोपनीयता उल्लङ्घन वा असन्तुलित डिजिटल प्रस्तुतीकरणले सामाजिक तनाव बढाउन, व्यक्तिको प्रतिष्ठामा क्षति पुर्‍याउन र पत्रकारिताप्रतिको सार्वजनिक विश्वास कमजोर बनाउन सक्छ । विशेषगरी निर्वाचन, राजनीतिक आन्दोलन, हिंसा, वा संवेदनशील सामाजिक मुद्दाको रिपोर्टिङ गर्दा डिजिटल अधिकारको सवाल अझ गम्भीर बन्छ। यस्तो सन्दर्भमा पत्रकारको पेसागत जिम्मेवारी भनेको सार्वजनिक हित र व्यक्तिको अधिकारबीच सन्तुलन कायम गर्नु हो।

डिजिटल अधिकार सुनिश्चित गर्नु भनेको केवल कानुनको परिपालना गर्नु मात्र होइन, यो जिम्मेवार, नैतिक र सुरक्षित पत्रकारिताको अभ्यास हो। पत्रकारले आफ्नै डिजिटल सुरक्षाको ख्याल राख्नु, स्रोत र पीडितको सुरक्षा सुनिश्चित गर्नु, र डिजिटल

प्लेटफर्ममा हुने दुरुपयोगको आलोचनात्मक समीक्षा गर्नु यस दायित्वको अभिन्न हिस्सा हो । डिजिटल अधिकारको सम्मान र संरक्षण गर्दै गरिएको पत्रकारिता नै आजको डिजिटल युगमा सुरक्षित, जिम्मेवार र लोकतान्त्रिक पत्रकारिताको आधार हो ।

दैनिक रिपोर्टिङमा डिजिटल अधिकार सुनिश्चित गर्ने व्यवहारिक अभ्यास

■ गर्नुपर्ने कार्यहरू (DO's)

क) सूचनाको प्रमाणीकरणमा विशेष ध्यान दिनुहोस् ।

सामाजिक सञ्जाल, मेसेजिङ एप वा अनलाइन प्लेटफर्मबाट प्राप्त सूचना, तस्बिर वा भिडियो प्रयोग गर्नु अघि त्यसको स्रोत, मिति, स्थान र सन्दर्भ अनिवार्य रूपमा जाँच गर्नुहोस् । डिजिटल माध्यमको गति र दबाबका कारण प्रमाणीकरण प्रक्रियालाई छोट्याउनु हुँदैन ।

ख) सार्वजनिक हित र गोपनीयताको सन्तुलन कायम गर्नुहोस् ।

कुनै सूचना सार्वजनिक रूपमा उपलब्ध छ भन्दैमा त्यसलाई समाचार बनाउनु उपयुक्त नहुन सक्छ । व्यक्तिको निजी जीवन, पीडितको पहिचान वा संवेदनशील विवरण सार्वजनिक गर्दा त्यसको आवश्यकताबारे आलोचनात्मक रूपमा सोच्नुहोस् ।

ग) स्रोत र पीडितको डिजिटल सुरक्षा सुनिश्चित गर्नुहोस् ।

संवेदनशील विषयमा रिपोर्टिङ गर्दा स्रोत वा पीडितको पहिचान गोप्य राख्नु, सुरक्षित डिजिटल माध्यम प्रयोग गर्नु र अनावश्यक डिजिटल ट्रेस नछोड्ने अभ्यास अपनाउनु अत्यन्त आवश्यक हुन्छ । यसले स्रोतको शारीरिक तथा डिजिटल सुरक्षाको संरक्षण गर्नुका साथै पत्रकार र सञ्चार माध्यमप्रति विश्वास कायम गर्न सहयोग पुर्‍याउँछ ।

घ) आधिकारिक र खुला डिजिटल स्रोतको प्रयोग बढाउनुहोस् ।

सरकारी वेबसाइट, खुला डाटा पोर्टल, निर्वाचन आयोगका डिजिटल अभिलेख तथा अन्य विश्वसनीय सार्वजनिक स्रोतको प्रयोगले समाचारको तथ्यगत आधार बलियो बनाउँछ । यस्ता स्रोतले सूचना प्रमाणित गर्न सहज बनाउनुका साथै मिथ्या वा भ्रामक सूचना र अडकलमा आधारित रिपोर्टिङको जोखिम घटाउँछन् ।

ङ) मिथ्या सूचना र दुष्प्रचारको सक्रिय खण्डन गर्नुहोस् ।

मिथ्या वा भ्रामक सूचना वा योजनाबद्ध दुष्प्रचार देखिएमा त्यसलाई जस्ताको तस्तै पुनः प्रसारण गर्नुको सट्टा तथ्य, प्रमाण र विश्वसनीय स्रोतका आधारमा सन्दर्भसहित खण्डन गर्नु पत्रकारको जिम्मेवारी हो । यसले सूचना अखण्डताको संरक्षण गर्नुका साथै सार्वजनिक बहसलाई सही दिशामा डोऱ्याउन मद्दत गर्छ ।

च) डिजिटल प्लेटफर्ममा पेसागत आचारसंहिता पालना गर्नुहोस् ।

व्यक्तिगत सामाजिक सञ्जाल प्रयोग गर्दा पनि पत्रकारको सार्वजनिक र पेसागत भूमिकालाई ध्यानमा राख्दै जिम्मेवार, सन्तुलित र मर्यादित व्यवहार गर्न आवश्यक हुन्छ । अनलाइन अभिव्यक्तिले पेसागत निष्पक्षता र विश्वसनीयतामाथि असर पार्न सक्ने भएकाले डिजिटल प्लेटफर्ममा आचारसंहिताको पालना थप महत्त्वपूर्ण हुन्छ ।

छ) भाषा र प्रस्तुतीकरणप्रति सचेत रहनुहोस् ।

संवेदनशील राजनीतिक विषयवस्तु तथा निर्वाचन रिपोर्टिङमा प्रयोग हुने भाषा, हेडलाइन, क्याप्सन र भिजुअल सामग्रीले सार्वजनिक धारणा निर्माणमा गहिरो प्रभाव पार्छ । त्यसैले उत्तेजक, पूर्वाग्रही वा भ्रम सिर्जना गर्ने प्रस्तुतीकरणबाट बच्दै तथ्यमा आधारित, सन्तुलित र सन्दर्भसहितको प्रस्तुति दिनु सूचना अखण्डता र जिम्मेवार पत्रकारिताका लागि अत्यावश्यक हुन्छ ।

■ गर्न नहुने कार्यहरू (DON'Ts)

क) पुष्टि नभएको डिजिटल सामग्रीमा आधारित समाचार नबनाउनुहोस् ।

सामाजिक सञ्जाल वा अनलाइन प्लेटफर्ममा भाइरल भएको छ भन्दैमा कुनै सामग्रीको सत्यता, स्रोत र सन्दर्भ नजाँची समाचार बनाउनु सूचना अखण्डतामाथि प्रत्यक्ष प्रहार हो । यस्तो अभ्यासले मिथ्या वा भ्रामक सूचना र दुष्प्रचार फैलिन सहयोग पुर्याउनुका साथै पत्रकारिताको विश्वसनीयता र नागरिकको सूचनाको अधिकारलाई गम्भीर रूपमा क्षति पुर्‌याउँछ ।

ख) क्लिक र भ्युजको लोभमा गोपनीयता उल्लङ्घन नगर्नुहोस् ।

ट्राफिक बढाउने वा डिजिटल प्रतिस्पर्धामा अघि बढ्ने नाममा पीडितको तस्बिर, नाम वा निजी विवरण प्रयोग गर्नु अनैतिक मात्र होइन, पीडितको गोपनीयता र गरिमामाथि आघात हो। यस्ता सामग्रीले पत्रकारिताप्रति सार्वजनिक विश्वास कमजोर बनाउनुका साथै डिजिटल अधिकार, विशेषतः गोपनीयताको अधिकार, उल्लङ्घन हुने जोखिम बढाउँछ ।

ग) व्यक्तिगत डाटा स्वेच्छाचारी रूपमा प्रयोग नगर्नुहोस् ।

व्यक्तिको निजी जानकारी तथा तथ्याङ्क जस्तै फोन नम्बर, ठेगाना, निजी सन्देश, स्क्रिनसट वा लिंक सामग्री प्रयोग गर्दा त्यसको सार्वजनिक महत्त्व, सहमति र आवश्यकता स्पष्ट हुनुपर्छ । सम्भावित कानुनी, नैतिक र सुरक्षा जोखिमको मूल्याङ्कन नगरी यस्ता डाटा प्रयोग गर्दा गोपनीयता हनन् हुनुका साथै पत्रकार र सञ्चार माध्यमलाई दीर्घकालीन उत्तरदायित्व र जोखिममा पार्न सक्छ ।

घ) घृणात्मक वा विभाजनकारी अभिव्यक्तिलाई सामान्यीकरण नगर्नुहोस् ।

घृणात्मक, विभाजनकारी वा उत्तेजक अभिव्यक्तिलाई सन्दर्भ, तथ्यगत स्पष्टता र आलोचनात्मक व्याख्या बिना प्रस्तुत गर्नु दुष्प्रचारलाई अप्रत्यक्ष रूपमा वैधता दिनु सरह हो । यस्तो सामग्रीको लापरवाह रुपमा गरिएको प्रस्तुतीकरणले सामाजिक

ध्रुवीकरण बढाउनुका साथै सूचना अखण्डता कमजोर बनाउँछ र मिडियाको नैतिक जिम्मेवारी तथा सार्वजनिक विश्वासमा गम्भीर असर पार्न सक्छ।

ङ) स्रोतको सहमति बिना डिजिटल संवाद सार्वजनिक नगर्नुहोस्।

निजी च्याट, इमेल, अडियो वा भिडियो रेकर्डिङजस्ता डिजिटल संवाद प्रयोग गर्दा स्रोतको स्पष्ट सहमति र सुरक्षा सुनिश्चित गर्नु पत्रकारको आधारभूत कर्तव्य हो। सहमति बिना यस्ता सामग्री सार्वजनिक गर्दा स्रोतको गोपनीयता र सुरक्षामा खतरा उत्पन्न हुनुका साथै पत्रकार र सञ्चार माध्यम स्वयं कानुनी, नैतिक र पेसागत जोखिममा पर्न सक्छन्।

च) व्यक्तिगत र पेसागत पहिचानबीचको सीमा नतोड्नुहोस्।

पत्रकारको व्यक्तिगत सामाजिक सञ्जाल गतिविधि र पेसागत भूमिकाबीच स्पष्ट सीमा कायम नराख्दा रिपोर्टिङको निष्पक्षता र विश्वसनीयतामाथि प्रश्न उठ्न सक्छ। व्यक्तिगत अभिव्यक्तिले राजनीतिक झुकाव वा पूर्वाग्रह झल्किने अवस्था सिर्जना गरेमा त्यसले सम्पादकीय स्वतन्त्रता, पेसागत मर्यादा र सार्वजनिक विश्वासलाई कमजोर पार्न सक्छ।

छ) डिजिटल जोखिमलाई सामान्य रुपमा लिई बेवास्ता नगर्नुहोस्।

अनलाइन धम्की, ट्रोलिङ, लक्षित दुष्प्रचार वा साइबर आक्रमणलाई व्यक्तिगत समस्या मानेर चुप लाग्नु दीर्घकालीन रूपमा जोखिमपूर्ण हुन्छ। यस्ता घटनालाई संस्थागत रूपमा अभिलेखीकरण गर्नु, कानुनी र सुरक्षा संयन्त्रमार्फत सम्बोधन गर्नु तथा सहकर्मी र संस्थाको सहयोग खोज्नु पत्रकारको डिजिटल सुरक्षा, मानसिक स्वास्थ्य र पेसागत स्वतन्त्रताको संरक्षणका लागि आवश्यक हुन्छ।

१.४ डिजिटल अधिकार बेवास्ता गर्दा पत्रकारले सामना गर्न सक्ने कानुनी दायित्व र सजाय

डिजिटल अधिकारको सम्मान नगरी गरिएको रिपोर्टिङले पत्रकारलाई नैतिक

आलोचनासँगै कानुनी कारबाही तथा संस्थागत अनुशासनात्मक कारबाहीको जोखिममा समेत पार्न सक्छ। नेपालमा पत्रकारिताको अभ्यास नेपालको संविधान, कानुन र पेसागत आचारसंहिताको दायराभित्र रहनुपर्छ। त्यसैले, विद्यमान कानुनी व्यवस्था अनुसार डिजिटल माध्यमबाट हुने गैर जिम्मेवारीपूर्ण क्रियाकलापका लागि पत्रकार पनि उत्तरदायी हुन सक्छन्।

विद्धुतीय कारोबार ऐन, २०६३[3] को दफा ४७ ले "कम्प्युटर, इन्टरनेट लगायतका विद्युतीय सञ्चार माध्यमहरुमा प्रचलित कानुनले प्रकाशन तथा प्रदर्शन गर्न नहुने भनी रोक लगाएका सामग्रीहरु वा सार्वजनिक नैतिकता, शिष्टाचार विरुद्धका सामग्री वा कसैप्रति घृणा वा द्वेष फैलाउने वा विभिन्न जात जाति र सम्प्रदाय बीचको सुमधुर सम्बन्धलाई खलल पार्ने किसिमका सामग्रीहरु प्रकाशन वा प्रदर्शन गर्ने, महिलालाई जिस्क्याउने, हैरानी गर्ने, अपमान गर्ने वा यस्तै अन्य कुनै किसिमको अमर्यादित कार्य गर्ने वा गर्न लगाउने व्यक्तिलाई एक लाख रुपैयाँसम्म जरिबाना वा पाँच वर्षसम्म कैद वा दुवै सजाय हुनेछ" भन्ने व्यवस्था गरेको छ।

त्यस्तै, मुलुकी अपराध संहिताको[4] दफा ३०६ मा "अरुको इज्जतमा धक्का पुर्‍याउने नियतले वा धक्का पुग्न सक्छ भन्ने जानीजानी वा विश्वास गर्ने मनासिब कारण भई लेखेर, आचरण वा आकार वा चिह्न वा प्रचार प्रसारद्वारा वा अरु कुनै किसिमबाट प्रत्यक्ष वा अप्रत्यक्ष रूपले त्यस्तो व्यक्तिलाई अरुको दृष्टिमा निजको व्यक्तिगत चरित्र, आचरण, नैतिकता वा ख्यातिलाई होच्याउने गरी चरित्र हत्या गरेमा वा निजको शरीर सामान्यतः घृणित अवस्थामा छ भन्ने अरुलाई विश्वास पुग्ने गरी दोष लगाएमा वा त्यस्तो दोष लगाएको कुरा प्रचार, प्रसार वा प्रकाशन गरेमा वा कसैको बेइज्जती हुने साधनको रूपमा प्रयोग गरिएको कुनै चिज जानीजानी बिक्री वा वितरण गरेमा बेइज्जती गरेको मानिने" र सो गरेमा निजलाई "दुई वर्षसम्म कैद वा बिस हजार रुपैयाँसम्म जरिबाना वा दुवै सजाय हुनेछ भन्ने व्यवस्था गरिएको छ। यसका साथै विद्युतीय वा अन्य आम सञ्चार माध्यमबाट बेइज्जती गरे वा गराएमा

3 https://www.nrb.org.np/contents/uploads/2021/07/.pdf

4 https://www.nrb.org.np/contents/uploads/

त्यस्तो सजायमा थप एक वर्षसम्म कैद र दश हजार रुपैयाँसम्म जरिबाना हुनेछ" भनी दफा ३०७ मा उल्लेख गरिएको छ।

त्यसैगरी, प्रेस काउन्सिल नेपालले पत्रकार आचारसंहिता, २०७३ को दफा १३ मा "अनलाइन सञ्चारमाध्यमबाट समाचार तथा समाचार सामग्रीको प्रकाशन-प्रसारण वा बाह्य लिङ्कहरूलाई प्रकाशित गर्नुअघि तिनको विश्वसनीयता परीक्षण गर्नुपर्नेछ र प्रकाशित वा प्रसारित भएका सामग्री अनलाइनमा रहिरहने व्यवस्था गर्नुपर्दछ । तर मुलुकको सार्वभौमसत्ता, भौगोलिक अखण्डता, राष्ट्रिय सुरक्षा, सार्वजनिक स्वास्थ्य र सुरक्षा, सामाजिक सद्भाव जस्ता गम्भीर असर पर्ने सामग्री हटाउन काउन्सिलले निर्देशन दिन सक्नेछ" भन्ने व्यवस्था छ। साथै, दफा ६ मा यस आचारसंहिता उल्लङ्घन गरेमा सोसम्बन्धी उजुरी तथा कारबाही प्रक्रियाको व्यवस्था गर्दै दफा ७ मा कारबाही तथा निर्णयको समेत व्यवस्था गरेको छ।[5]

यसर्थ, डिजिटल अधिकारको सम्मान गर्नु नैतिक वा पेसागत दायित्व मात्र नभई, कानुनी जोखिम न्यूनीकरण गर्ने आवश्यक अभ्यास पनि हो। तथ्य प्रमाणीकरण, गोपनीयताको संरक्षण, सन्तुलित प्रस्तुतीकरण र डिजिटल सुरक्षा अपनाउँदै गरिएको पत्रकारिता कानुनी रूपमा सुरक्षित, पेसागत रूपमा विश्वसनीय र लोकतान्त्रिक रूपमा जिम्मेवार पत्रकारिता हो।

5 https://www.presscouncilnepal.gov.np/np/wp-content/uploads/2019/09/code-of-conduct-2076.pdf

परिच्छेद २

डिजिटल सुरक्षा र सुरक्षात्मक उपायहरु

डिजिटल प्रविधिको तीव्र विस्तारसँगै पत्रकारिताको अभ्यास, पहुँच र प्रभाव उल्लेखनीय रूपमा बढेको छ। तर यही डिजिटल रूपान्तरणका कारण पत्रकारहरूले नयाँ र जटिल प्रकारका जोखिम तथा खतराहरूको सामना समेत गर्नु परेको छ। आजका पत्रकारहरूले ह्याकिङ, डाटा तथा स्रोत चोरी, अनधिकृत पहुँच, अनलाइन दुर्व्यवहार र धम्की, डिजिटल निगरानी, फिशिङ आक्रमण, मालवेयर, नक्कली वा छद्म पहिचानको दुरुपयोग, तथा डक्सिङजस्ता गम्भीर डिजिटल खतराहरू नियमित रूपमा भोग्नुपरेको छ। यस्ता जोखिमहरूले केवल पत्रकारको व्यक्तिगत सुरक्षा मात्र होइन, स्रोतको गोपनीयता, सम्पादकीय स्वतन्त्रता, र समग्रमा स्वतन्त्र तथा विश्वसनीय पत्रकारितामै प्रत्यक्ष असर पार्ने गर्दछ।

डिजिटल खतराहरू प्रायः अदृश्य, प्रविधिमैत्री र सीमापार प्रकृतिका हुने भएकाले तिनको पहिचान, मूल्याङ्कन र व्यवस्थापन झन् चुनौतीपूर्ण बन्दै गएको छ। त्यसैले डिजिटल सुरक्षा र साइबर सुरक्षालाई पत्रकारिताको वैकल्पिक सीपका रूपमा मात्र होइन, पेसागत जिम्मेवारी र आवश्यक आधारभूत दक्षताका रूपमा बुझिनु आवश्यक छ। खतरा कसरी उत्पन्न हुन्छ, कसको तर्फबाट आउन सक्छ, कुन अवस्थामा जोखिम बढी हुन्छ र त्यसको सम्भावित प्रभाव कति गम्भीर हुन सक्छ भन्ने कुराको स्पष्ट बुझाई बिना प्रभावकारी रोकथाम र प्रतिक्रिया सम्भव हुँदैन।

यस परिच्छेदले पत्रकारहरूलाई डिजिटल सुरक्षाका आधारभूत अवधारणा, सम्भावित खतरा पहिचान गर्ने तरिका, जोखिम न्यूनीकरणका उपाय, र डिजिटल आक्रमण वा दुर्व्यवहारको अवस्थामा अपनाउनुपर्ने व्यावहारिक उपायहरू उल्लेख गरेको छ। साथै, यसले सुरक्षित डिजिटल अभ्यास, स्रोत र सूचनाको गोपनीयता संरक्षण, र अभिव्यक्ति स्वतन्त्रता तथा सूचनाको अधिकारको रक्षा गर्दै जिम्मेवार र सुरक्षित पत्रकारिता अभ्यास गर्न आवश्यक ज्ञान र सीप सुदृढ गर्ने उद्देश्य राख्दछ।

२.१ पत्रकारहरूले सामना गर्ने प्रमुख डिजिटल खतरा र त्यसलाई सम्बोधनका उपाय

आक्रमण हुनु अघि सुरक्षित हुनका लागि अपनाउनुपर्ने न्यूनतम तयारी (Before Compromise Checklist)

- खाता पुनः प्राप्ति (Account Recovery) का लागि प्रयोग गरिएको इमेल सुरक्षित छ कि छैन ?
- पुनः प्राप्ति फोन नम्बर (Recovery Phone) आफ्नो नाममा दर्ता गरिएको सिमकार्ड हो कि होइन, र त्यस नम्बरमा आफ्नो मात्र पहुँच छ कि अन्य व्यक्तिको पनि पहुँच छ ?
- बहुतह प्रमाणीकरण (2FA/MFA) का ब्याकअप कोडहरू सुरक्षित रूपमा अफलाइनमा भण्डारण गरिएको छ कि छैन ?
- आफ्नो खातामा अन्य व्यक्तिको पहुँच भएमा आफ्ना गोप्य स्रोत वा संवेदनशील सम्पर्क तथा सूचनाहरू कत्तिको जोखिममा पर्न सक्छन् भन्ने विषयमा आवश्यक मूल्याङ्कन गरिएको छ कि छैन ?
- स्रोतको पहिचान लुकाउने (masking) र न्यूनतम जानकारी सङ्कलनजस्ता अभ्यासहरू अपनाइएको छ कि छैन ?

क. ह्याकिङ (Hacking)

ह्याकिङ भन्नाले इमेल, सामाजिक सञ्जाल, क्लाउड स्टोरेज, वा अन्य डिजिटल खातामा अनधिकृत पहुँच प्राप्त गरी सूचना चोरी, परिवर्तन वा नष्ट गर्ने कार्यलाई जनाउँछ। यस्ता आक्रमणमार्फत आक्रमणकारीले पत्रकारको नाममा भ्रामक सामग्री पोस्ट गर्न, संवेदनशील स्रोतको पहिचान सार्वजनिक गर्न, वा अनुसन्धान सामग्रीमा हस्तक्षेप गर्न सक्छन्। ह्याकिङले पत्रकारको व्यक्तिगत सुरक्षा, पेसागत विश्वसनीयता र संस्थागत प्रतिष्ठामा नकारात्मक असर पार्न सक्छ । ह्याकिङका प्रारम्भिक सङ्केतहरुमा अपरिचित स्थान वा डिभाइसबाट गरिएको लगइनको सूचना आउनु, आफूले नगरेको अवस्थामा पासवर्ड परिवर्तन वा खातामा कुनै गतिविधि देखिनु, तथा शङ्कास्पद इमेल, फाइल वा लिङ्क प्राप्त हुनु पर्दछन्।

ह्याकिङको रोकथाम तथा सुरक्षा उपायहरु

- प्रत्येक महत्त्वपूर्ण डिजिटल खाताका लागि कम्तीमा १२ क्यारेक्टरभन्दा लामो, अक्षर, अङ्क र विशेष चिन्हको संयोजन भएको बलियो पासवर्ड प्रयोग गर्नुहोस्।
- एउटै पासवर्ड विभिन्न खातामा प्रयोग नगर्नुहोस्।
- पासवर्डहरू सुरक्षित रूपमा व्यवस्थापन गर्न पासवर्ड म्यानेजर प्रयोग गर्नुहोस्।
- सबै संवेदनशील डिजिटल खातामा Two-Factor Authentication (2FA) वा Multi-Factor Authentication (MFA) अनिवार्य रूपमा सक्रिय गर्नुहोस्।
- इमेलमार्फत प्राप्त लिङ्कमा सिधै क्लिक नगरी सम्बन्धित सेवाको आधिकारिक वेबसाइटमा गएर मात्र लगइन गर्नुहोस्।
- सार्वजनिक वाईफाई (Public Wi-Fi) प्रयोग गर्दा सकेसम्म संवेदनशील फाइल वा जानकारी आदानप्रदान नगर्नुहोस्।

- सार्वजनिक वाईफाई प्रयोग गरेर संवेदनशील काम गर्नै पर्ने अवस्थामा Virtual Private Network (VPN) प्रयोग गरी सुरक्षित रूपमा इन्टरनेट चलाउनुहोस्।
- समय-समयमा आफ्नो इमेल, सामाजिक सञ्जाल तथा क्लाउड सेवाको Active Sessions/Devices सूची जाँच गरी आफूले नचिनेका वा शङ्कास्पद डिभाइसहरूबाट log out वा revoke access गर्नुहोस्।
- आक्रमणकारीहरूले धेरैजसो इमेल अकाउन्ट ह्याक गरेपछि गोप्य रूपमा सबै इमेल अर्को ठेगानामा auto-forward हुने (forwarding rule) बनाएका हुन सक्छन्। त्यसैले इमेलको Settings तथा Forwarding / Filters/Rules खण्ड नियमित रूपमा जाँच गर्नुहोस् र आफूले सेट नगरेका नियमहरू तुरुन्तै हटाउनुहोस्।

ख. डाटा चोरी (Data Theft)

डाटा चोरी भन्नाले कम्प्युटर वा डिभाइसका सामग्री, सम्पर्क सूची, स्रोतसम्बन्धी विवरण वा व्यक्तिगत डाटामा अनधिकृत रूपमा पहुँच प्राप्त गर्ने, त्यस्ता सामग्रीको प्रतिलिपि बनाउने वा सार्वजनिक गर्ने कार्यलाई जनाउँछ। यस्तो जोखिम विशेषगरी खोज पत्रकारिता, भ्रष्टाचार, मानव अधिकार वा संवेदनशील राजनीतिक विषयमा काम गर्ने पत्रकारहरूका लागि अत्यन्त गम्भीर हुन्छ। डाटा चोरीका सङ्केतहरुमा आफूले नचिनेका एप वा फाइलहरु देखिनु, वा क्लाउड/ड्राइभमा सुरक्षित फाइलहरु आफैँ हराउनु, वा अनपेक्षित परिवर्तन हुनु, तथा संवेदनशील स्रोतसँगको निजी संवाद बाहिरिनु समावेश हुन्छन्।

डाटा चोरीको रोकथाम तथा सुरक्षाका उपायहरु

- ल्यापटप र मोबाइल फोनमा Full-Disk Encryption सक्रिय गर्नुहोस्।
- अपरेटिङ सिस्टम तथा सबै एप्लिकेसनहरू नियमित रूपमा अद्यावधिक राख्नुहोस्।

- विश्वसनीय एण्टी-भाइरस वा एण्टी-मालवेयर सफ्टवेयर प्रयोग गर्नुहोस् ।
- संवेदनशील डाटाको नियमित रूपमा इन्क्रिप्टेड ब्याक अप सुरक्षित स्थानमा राख्नुहोस् ।
- स्रोतहरूसँग संवाद गर्दा End-to-End Encrypted मेसेजिङ एप प्रयोग गर्नुहोस् ।

ग. अनलाइन दुर्व्यवहार (Online Harassment)

अनलाइन दुर्व्यवहार अन्तर्गत धम्की, अपमानजनक टिप्पणी, गालीगलौज, लैङ्गिक वा पहिचानमा आधारित आक्रमण, र सङ्गठित डिजिटल आक्रमण (dogpiling) पर्दछन् । यसका साथै सामाजिक सञ्जालमा गरिएका पुराना पोस्ट, लाइक, टिप्पणी वा प्रतिक्रियाहरू सन्दर्भविहीन रूपमा प्रयोग गरी अनलाइन दुर्व्यवहार हुन सक्छ । यस्तो दुर्व्यवहारले पत्रकारको मानसिक स्वास्थ्यमा असर पार्नुका साथै स्वनियन्त्रण (self-censorship) बढाउने र पेसागत जोखिम निम्त्याउने सम्भावना हुन्छ । कसैबाट बारम्बार धम्की, गालीगलौज वा अपमानजनक सन्देश आउनु (जुन प्राय जसो अपरिचित वा नक्कली खाताबाट आउँछन्); एउटै सामग्रीमा धेरै खाताबाट एकै समयमा समान शैलीका कमेन्टहरू आउनु (संयोजित आक्रमण); व्यक्तिगत जानकारी सहमतिबिना सार्वजनिक गरिनु तथा पुराना फोटो वा भिडियो सन्दर्भ परिवर्तन गरी दुष्प्रचारका लागि प्रयोग गरिनु अनलाइन दुर्व्यवहारका उदाहरण हुन् ।

अनलाइन दुर्व्यवहारको रोकथाम तथा सुरक्षा उपाय

- सामाजिक सञ्जालमा उपलब्ध गोपनीयता (Privacy) सेटिङहरू सक्रिय गर्नुहोस् ।
- व्यक्तिगत जानकारी सार्वजनिक नहोस् भन्ने चाहनुहुन्छ भने गोपनीयता सेटिङहरू नियमित रूपमा समीक्षा र अद्यावधिक गर्नुहोस् ।

- आफ्ना पोस्ट कसले हेर्न, टिप्पणी गर्न वा प्रत्यक्ष सन्देश पठाउन सक्छ भन्ने कुरा गोपनीयता सेटिङमार्फत नियन्त्रण गर्नुहोस्।
- आफ्नो नाम वा उपनाम प्रयोग गरी अनलाइनमा सामग्री फैलाइएको छ कि छैन भनी Google Alert सेट गरी निगरानी गर्नुहोस्।
- आपत्तिजनक, दुर्व्यवहारजन्य वा शङ्कास्पद खाताहरूलाई सम्बन्धित प्लेटफर्ममा रिपोर्ट गर्नुहोस् र सोलाई ब्लक गर्नुहोस्।
- समय-समयमा आफ्नो डिजिटल footprint समीक्षा र आवश्यक परे सफाइ (cleanup) गर्नुहोस्।

सामाजिक सञ्जालका एल्गोरिदमले उच्च संलग्नता (engagement) भएका सामग्रीलाई अझ बढी फैलाउने भएकाले, दुर्व्यवहारपूर्ण सामग्रीमा प्रतिक्रिया जनाउँदा (reply, like, quote) आक्रमणलाई बढावा दिन सक्छ भन्ने कुरामा सचेत रहन आवश्यक छ।

घ. फिशिङ (Phishing)

फिशिङ आक्रमणमा नक्कली इमेल, सन्देश वा वेबसाइट प्रयोग गरी झुक्क्याएर पासवर्ड, OTP, वा अन्य संवेदनशील जानकारी प्राप्त गर्ने प्रयास गरिन्छ। यस्ता आक्रमणहरुले ह्याकिङ र डाटा चोरीका लागि बाटो खोल्ने काम गर्दछ। अत्यधिक आतुरता, डर, वा आकस्मिक निर्णय गर्न लगाउने भाषा (जस्तै 'तुरुन्तै लगइन गर्नुहोस्', 'तपाईंको खाता ब्लक हुन सक्छ'), इमेल वा वेबसाइटको URL मा सामान्य अक्षरगत परिवर्तन (जस्तै nabil.com को सट्टा nabl.com) वा पुरस्कार, विदेश भ्रमणका अवसर देखाउँदै व्यक्तिगत, वित्तीय वा संवेदनशील जानकारी माग्ने अनुरोधहरू फिशिङका सङ्केत हुन सक्छन्।

फिशिङबाट सुरक्षित रहने उपाय

- कुनै पनि लिङ्कमा क्लिक गर्नु अघि URL सावधानीपूर्वक जाँच गर्नुहोस्।
- इमेल, सन्देश वा सामाजिक सञ्जालमार्फत प्राप्त लिङ्क प्रयोग नगरी वेब ब्राउजरमा आधिकारिक वेबसाइटको ठेगाना सिधै टाइप गरी लगइन गर्नुहोस्।
- सबै महत्त्वपूर्ण डिजिटल खातामा Two-Factor Authentication (2FA) वा Multi-Factor Authentication (MFA) सक्रिय गर्नुहोस्। तर, 2FA/MFA सक्रिय गर्दा प्लेटफर्मले उपलब्ध गराउने backup codes (recovery codes) सुरक्षित रूपमा डाउनलोड गरी अफलाइनमा सुरक्षित रुपमा राख्नुहोस्, ताकि मोबाइल फोन हराएमा, चोरी भएमा, वा 2FA एपमा पहुँच गुम्यो भने पनि आफ्नो खातामा पहुँच पुनः प्राप्त गर्न गाह्रो नहोस्।
- अपरिचित वा शङ्कास्पद लिङ्क, attachment वा फाइल नखोल्नुहोस्।
- कुनै पनि फाइल वा लिङ्क खोल्नु अघि VirusTotal6 जस्ता निःशुल्क सुरक्षा उपकरण प्रयोग गरी सुरक्षा जाँच गर्नुहोस्।
- शङ्कास्पद इमेल वा सन्देशका बारेमा सम्बन्धित सेवा प्रदायकलाई रिपोर्ट गर्नुहोस् र त्यस्ता इमेल वा सन्देशलाई delete गर्नुहोस्।

ङ. मालवेयर (Malware)

मालवेयर भनेको कसैको जानकारी बिना डिभाइसमा प्रवेश गरी डाटा चोरी गर्ने, निगरानी गर्ने वा डिभाइसलाई नियन्त्रणमा लिने हानिकारक सफ्टवेयर हो। यस्तो सफ्टवेयरले पत्रकारको गतिविधि ट्र्याक गर्न र संवेदनशील जानकारी बाहिर पठाउन

6 https://www.virustotal.com/gui/home/upload

सक्छ। डिभाइस असामान्य रूपमा ढिलो हुनु, पटक-पटक क्र्यास हुनु, अनावश्यक पप-अप देखिनु वा सेटिङहरू आफै परिवर्तन हुनु मालवेयरका सम्भावित सङ्केत हुन्।

मालवेयरबाट रोकथाम तथा सुरक्षा उपाय

- विश्वसनीय एण्टी-भाइरस वा एण्टी-मालवेयर सफ्टवेयर प्रयोग गरी त्यसलाई नियमित रूपमा अद्यावधिक गर्नुहोस्।
- अपरेटिङ सिस्टम र प्रयोग भइरहेका एपहरू सधैँ नवीनतम संस्करणमा अद्यावधिक राख्नुहोस्।
- एपहरू डाउनलोड गर्दा App Store वा Play Store जस्ता आधिकारिक स्रोतहरूबाट मात्रै डाउनलोड गर्नुहोस्, अन्य स्रोतबाट एप डाउनलोड नगर्नुहोस्।

च. नक्कली पहिचान (Impersonation)

नक्कली पहिचान अन्तर्गत कसैको नाम, फोटो वा संस्थागत पहिचान प्रयोग गरी भ्रम फैलाउने, कसैलाई बदनाम गर्ने वा उक्त पहिचानको व्यक्तिविरूद्ध अविश्वास सिर्जना गर्ने उद्देश्यले झूटा खाता, सन्देश वा सामग्री सिर्जना गरिन्छ। आफ्नै नाम र फोटो प्रयोग गरिएको अर्को खाता फेला पर्नु वा संस्थाको नाम प्रयोग गरी भ्रामक सामग्री प्रकाशन हुनु नक्कली पहिचान (impersonation) का सङ्केत हुन्।

पहिचान दुरूपयोगको रोकथाम तथा सुरक्षा उपाय

- समय-समयमा सामाजिक सञ्जालमा आफ्नो नाम खोजी गरी नक्कली वा शङ्कास्पद खाताहरूको पहिचान गर्नुहोस्।
- पहिचान गरिएका नक्कली खाताहरूलाई तत्काल सम्बन्धित प्लेटफर्ममा रिपोर्ट गर्नुहोस्।

- आवश्यक परे आधिकारिक च्यानलमार्फत नक्कली खाताको जानकारी सार्वजनिक गरी अरुलाई पनि सूचित गर्नुहोस्।

छ. डक्सिङ (Doxxing)

डक्सिङ भनेको कसैको निजी जानकारीहरू जस्तै घरको ठेगाना, व्यक्तिगत फोन नम्बर, परिवारसम्बन्धी विवरणहरू अनलाइनमा सार्वजनिक गरिनु हो । यसले शारीरिक, मानसिक तथा पारिवारिक सुरक्षामा प्रत्यक्ष खतरा उत्पन्न गर्छ। इन्टरनेटमा निजी जानकारी सार्वजनिक हुनु, वा सो जानकारी प्रयोग गरी धम्की, तर्साउने वा पछ्याउने गतिविधि हुनु डक्सिङका सङ्केतहरू हुन्।

डक्सिङ रोकथाम तथा सुरक्षा उपाय

- पुराना वा अनावश्यक अनलाइन खाताहरू बन्द गर्नुहोस् वा निष्क्रिय बनाउनुहोस्।
- व्यक्तिगत जानकारी भएका वेबसाइटहरूबाट आफ्नो विवरण हटाउन प्रयास गर्नुहोस्।
- सार्वजनिक Wi-Fi प्रयोग गर्दा सधैँ VPN (Virtual Private Network) प्रयोग गर्नुहोस्।
- संवेदनशील व्यक्तिगत जानकारी साझा गर्दा अत्यन्त सतर्कता अपनाउनुहोस्।

ज. अनधिकृत पहुँचबाट अकाउन्ट नियन्त्रणमा लिने

अकाउन्ट नियन्त्रण भन्नाले कसैको इमेल, सामाजिक सञ्जालको खाता वा अन्य डिजिटल सेवाका खातामा अनधिकृत पहुँच प्राप्त गरी त्यसको नियन्त्रण लिने कार्यलाई जनाउँछ। यस्तो आक्रमणपछि आक्रमणकारीले पत्रकारको नाममा झुटा सन्देश पठाउन, भ्रामक सामग्री पोस्ट गर्न, स्रोतहरुसँगको निजी संवाद पढ्न वा

मेटाउन, र पत्रकारको डिजिटल पहिचानको दुरुपयोग गर्न सक्छन् । अकाउन्ट नियन्त्रणका प्रारम्भिक सङ्केतहरुमा बारम्बार आफूले नगरेको लगइन वा लगआउट हुनु, पासवर्ड वा रिकभरी इमेल परिवर्तन भएको सूचना आउनु, आफूले नपठाएका सन्देशहरू पठाइएको देखिनु, वा सामाजिक सञ्जाल प्रोफाइलको सेटिङ आफैँ परिवर्तन हुनु पर्दछन् ।

अकाउन्ट नियन्त्रणको रोकथाम तथा सुरक्षा उपायहरू

- इमेल, Facebook, WhatsApp लगायत सबै महत्त्वपूर्ण खातामा 2FA/MFA अनिवार्य रूपमा सक्रिय गर्नुहोस् । सम्भव भएसम्म SMS भन्दा Authenticator App प्रयोग गर्नु सुरक्षित हुन्छ ।
- अकाउन्ट रिकभरी इमेल र फोन नम्बर अद्यावधिक र सुरक्षित राख्नुहोस् ।
- सामाजिक सञ्जालमा "Login alerts" वा "Security alerts" जस्ता सुरक्षा सूचना सेटिङ सक्रिय गर्नुहोस् ।
- अकाउन्टमा प्रयोग भएका डिभाइस र सेसनहरू नियमित रूपमा समीक्षा गरी अपरिचित डिभाइस तुरुन्तै हटाउनुहोस् ।

झ. सिम-स्वाप आक्रमण (SIM swap)

सिम-स्वाप आक्रमणमा आक्रमणकारीले मोबाइल सेवा प्रदायकलाई झुक्क्याएर अरुको मोबाइल नम्बर आफ्नो नियन्त्रणमा लिन्छ । त्यसपछि SMS आधारित OTP, पासवर्ड रिसेट कोड, वा अकाउन्ट रिकभरी सूचना आक्रमणकारीसम्म पुग्छ, जसबाट इमेल, सामाजिक सञ्जाल, वा बैंकिङ अकाउन्ट समेत ह्याक हुन सक्छन् । डिजिटल सुरक्षा दृष्टिले यो अत्यन्तै गम्भीर खतरा हो तर यसको बारेमा चर्चा भने कम हुने गरेको छ । सिम-स्वाप आक्रमणका सङ्केतहरूमा अचानक मोबाइल नेटवर्क नआउनु, कल वा SMS नजानु, "No service" देखिनु, वा आफ्नो नम्बर प्रयोग गरेर अकाउन्ट रिकभरी प्रयास भएको सूचना आउनु पर्दछन् ।

सिम–स्वाप भएमा के गर्ने ?

- आफ्नो नेटवर्क प्रदायकलाई तुरुन्तै कल गर्नुहोस् । यदि तपाईंले आफ्नो सिम पोर्ट गरिएको वा Porting Authorisation Code (PAC) अनुरोधको बारेमा अनावश्यक सन्देश वा इमेलहरू प्राप्त गर्नुभयो भने, वा तपाईंले अप्रत्याशित रूपमा मोबाइल नेटवर्क सेवा गुमाउनुभयो भने, तपाईंले आफ्नो प्रदायकलाई सूचित गर्नुपर्नेछ ।
- ठगी गर्ने व्यक्तिले अनलाइन वा फोन मार्फत पैसा स्थानान्तरण गर्ने प्रयास गर्न सक्ने भएकाले सकेसम्म चाँडो आफ्नो बैङ्कहरूलाई सूचित गर्नुहोस् ।

सिम–स्वाप विरुद्ध सुरक्षाका उपायहरु

- सकेसम्म अकाउन्ट प्रमाणीकरणका लागि SMS आधारित OTP भन्दा App-based authentication प्रयोग गर्नुहोस् ।
- मोबाइल नम्बर सार्वजनिक रूपमा (सोसल मिडिया बायो, वेबसाइट, प्रोफाइल) राख्न आवश्यक नभए हटाउनुहोस् ।

ञ. मोबाइल फोन निगरानी (Mobile Phone Surveillance)

मोबाइल फोन पत्रकारको सबैभन्दा संवेदनशील उपकरण हो किनकि यसमा कसलाई फोन गर्नुभयो वा कस कसको फोन आयो भन्ने जानकारी, म्यासेज/टेक्स्ट, स्रोतसँगको संवाद, फोटो, लोकेशन, नोट लगायतका धेरै महत्त्वपूर्ण विवरणहरू हुन्छन् । त्यसैले पत्रकार लक्षित आक्रमणमा आक्रमणकारीले ल्यापटपभन्दा पहिले मोबाइल फोनलाई लक्ष्य बनाउने सम्भावना बढी हुन्छ । यस्ता निगरानी प्रविधिहरू महँगा भए पनि उच्च-जोखिम रिपोर्टिङ (राजनीति, भ्रष्टाचार, मानव अधिकार) गर्ने पत्रकारहरूका लागि सम्भाव्य खतरा हुन् । मोबाइल निगरानीका सामान्य सङ्केतहरूमा फोन बारम्बार आफैँ लगआउट हुनु, ब्याट्री असामान्य रूपमा छिटो सकिनु, फोन अत्यधिक तातिनु, डाटा प्रयोग अचानक बढ्नु, वा फोन सुस्त चल्नु पर्दछन् ।

मोबाइल निगरानीबाट जोगिने उपायहरू

- मोबाइल अपरेटिङ सिस्टम र एपहरू सधैँ अद्यावधिक राख्नुहोस् ।
- आधिकारिक App Store वा Play Store बाहेकका स्रोतबाट एप इन्स्टल नगर्नुहोस् ।
- फोनमा Screen lock (PIN/Password/Biometric) अनिवार्य रूपमा प्रयोग गर्नुहोस् ।
- संवेदनशील संवादका लागि Signal जस्ता एन्ड-टू-एन्ड इन्क्रिप्टेड एप प्रयोग गर्नुहोस् ।
- अत्यधिक शङ्कास्पद गतिविधि देखिएमा फोन ब्याकअप लिएर factory reset गरी आवश्यक एप मात्र पुनः इन्स्टल गर्नुहोस् ।
- उच्च जोखिम रिपोर्टिङमा संलग्न हुँदाका समयमा व्यक्तिगत र कामका लागि अलग फोन प्रयोग गर्नु थप सुरक्षित अभ्यास हुन सक्छ ।

२.२ डिजिटल सुरक्षाका लागि निरोधात्मक उपायहरु (Preventive measures)

डिजिटल उपकरण तथा सञ्चार प्रक्रिया सुरक्षित नराखिएमा स्रोतको गोपनीयता, प्रेस स्वतन्त्रता र पत्रकारको व्यक्तिगत सुरक्षामै खतरा पर्छ । त्यसैले निम्न आधारभूत अभ्यास अनिवार्य छन् ।

क) उपकरणको सुरक्षा	
के गर्ने	**के नगर्ने**
ल्यापटप र मोबाइल उपकरणमा Full-disk encryption अनिवार्य रूपमा प्रयोग गर्ने । (ल्यापटपका लागि: BitLocker/ FileVault, मोबाइलका लागि: default encryption प्रयोग गर्न सकिन्छ)।	एउटै पासवर्ड सबै खाता वा सबै डिजिटल उपकरणमा प्रयोग नगर्ने।
कम्तीमा १२ अक्षर लामो, साना र ठूला अक्षर, सङ्ख्या र विशेष चिन्हको मिश्रण भएको बलियो पासवर्ड प्रयोग गर्ने।	डिजिटल उपकरण (मोबाइल, ल्यापटप) सार्वजनिक वा भिडभाड भएका स्थानमा निगरानी बिना छोड्ने कार्य नगर्ने।
प्रत्येक महत्त्वपूर्ण खाता (इमेल, CMS, सामाजिक सञ्जाल, बैङ्किङ, क्लाउड सेवा) का लागि फरक-फरक पासवर्ड प्रयोग गर्ने।	अनौपचारिक वा अविश्वसनीय स्रोतबाट एप्स वा सफ्टवेयर डाउनलोड/इन्स्टल नगर्ने।
Password Manager (जस्तै: Bitwarden, LastPass) प्रयोग गरी पासवर्ड सुरक्षित रूपमा भण्डारण गर्ने। Password Manager प्रयोग गर्दा त्यसलाई बलियो Master Password ले सुरक्षित गर्नुपर्छ र 2FA/MFA अनिवार्य रूपमा सक्रिय गर्नुपर्छ।	शङ्कास्पद वा अपरिचित पेनड्राइभ/USB जस्ता उपकरण प्रयोग नगर्ने ।

डाटा सुरक्षा, पहुँच नियन्त्रण र आकस्मिक जोखिम व्यवस्थापन सुनिश्चित गर्नका लागि सम्भव भएसम्म संस्थाद्वारा स्वीकृत (organization-approved) Password Manager मात्र प्रयोग गर्ने।	Password Manager मा प्रयोग गरिएको Master Password अरू कुनै खातामा प्रयोग नगर्ने।
Operating System (OS) र सबै एप्लिकेसनहरूका security update तथा patch समयमै गर्ने।	सुरक्षा जाँच प्रोटोकल नभएका (https://) वेबसाइटमा लग-इन विवरण (username/ password) तथा वैयक्तिक विवरण प्रविष्ट नगर्ने।
अन्य व्यक्तिको पेनड्राइभ वा USB उपकरण प्रयोग गर्दा सावधानी अपनाउने, आवश्यक परेमा मात्र प्रयोग गर्ने।	एक भन्दा बढी व्यक्तिले प्रयोग गर्ने वा सार्वजनिक कम्प्युटरमा व्यक्तिगत वा संस्थागत खाता log-in गरेर log-out नगरी छोड्ने कार्य नगर्ने।
पत्रकार तथा अन्य स्टाफका व्यक्तिगत उपकरणहरूमा पनि न्यूनतम सुरक्षा प्रोटोकल (पासवर्ड, स्क्रिन लक, encryption) लागू गर्ने।	उपकरणमा एन्टिभाइरस वा सुरक्षा सुविधा निष्क्रिय अवस्थामा राख्ने कार्य नगर्ने।
सार्वजनिक Wi-Fi प्रयोग गर्दा सकेसम्म संवेदनशील फाइल वा जानकारी आदान-प्रदान नगर्ने; अत्यावश्यक परेमा मात्र VPN प्रयोग गर्ने।	प्रयोग नभएको अवस्थामा वायरलेस वा ब्लुटुथ सेवालाई खुल्ला नराख्ने।

आफ्नो Windows कम्प्युटरमा सम्भावित निगरानी वा जासुसी सफ्टवेयर छ कि भनेर पहिचान गर्न Detekt जस्ता निःशुल्क उपकरण प्रयोग गरी समय-समयमा स्क्यान गर्ने।	रिपेयर पसलमा उपकरण नछोड्ने र मर्मतका लागि मात्र अनधिकृत सेवा केन्द्रमा नजाने।

ख) सुरक्षित सञ्चार

के गर्ने	के नगर्ने
संवेदनशील तथा गोप्य सन्देश आदान-प्रदान तथा अनुसन्धानसम्बन्धी संवादका लागि end-to-end encrypted एपहरू, जस्तै Signal, Wire, ProtonMail प्रयोग गर्ने।	प्राइभेसी स्क्रिन बिना सार्वजनिक स्थानमा संवेदनशील वा गोप्य कागजात/सूचना सबैले देख्ने गरी नहेर्ने।
उच्च-जोखिम वा संवेदनशील काममा disappearing messages / auto-delete जस्ता सुविधाहरू सक्रिय गर्ने।	अन्य व्यक्तिले सजिलै सुन्न सक्ने गरी सार्वजनिक स्थानमा गोप्य वा संवेदनशील टेलिफोन संवाद नगर्ने।
ल्यापटप र मोबाइलमा Privacy Screen (privacy filter) प्रयोग गर्ने।	Common वा कमजोर पासवर्ड प्रयोग नगर्ने।
महत्त्वपूर्ण डाटा encrypt गरिएको क्लाउड सेवा वा encrypt भएका external drive मा नियमित रूपमा ब्याकअप गर्ने।	असुरक्षित इमेल, SMS वा social media DM मार्फत अत्यन्त संवेदनशील सूचना आदान-प्रदान नगर्ने।
स्रोतसँगको सम्पर्क, आधिकारिक पत्राचार तथा संवेदनशील सूचनाका लागि छुट्टै पेसागत (कामको) इमेल खाता प्रयोग गर्ने, र व्यक्तिगत इमेल खाता किनमेल, मनोरञ्जन तथा सामाजिक कुराकानीका लागि मात्र प्रयोग गर्ने	कार्यालय वा संस्थाको आधिकारिक संवाद व्यक्तिगत र असुरक्षित प्लेटफर्ममा सीमाविहीन रूपमा गर्ने कार्य नगर्ने।

२.३ मेटाडाटा र मेटाडाटाको सुरक्षा

मेटाडाटा के हो ?

मेटाडाटा (Metadata) भन्नाले डाटाको बारेमा जानकारी दिने डाटालाई जनाउँछ। सरल शब्दमा, कुनै पनि डिजिटल फाइल वा सामग्रीको पहिचान र पृष्ठभूमि बताउने विवरण नै मेटाडाटा हो। यसमा उक्त फाइल के हो, कहिले सिर्जना गरियो, कसले तयार गर्‌यो, कहाँ र कुन उपकरणबाट बनाइयो, तथा कस्तो ढाँचामा सुरक्षित गरिएको छ भन्ने जानकारी समावेश हुन्छ।

फोटो, भिडियो, अडियो वा डिजिटल कागजातहरूमा साधारण प्रयोगकर्ताले नदेख्ने "मेटाडाटा" रहन्छ । यस्ता डाटाअन्तर्गत उक्त सामग्री उत्पादन गरिएको स्थान अर्थात् लोकेशन वा GPS, क्यामरा/फोनको मोडेल, खिचिएको मिति/समय, फाइल सम्पादन इतिहास आदि पर्दछन् । यस्ता मेटाडाटाले स्रोतको पहिचान वा स्थान खुलासा गरिदिन सक्छ, जसले स्रोत वा पत्रकार दुवैलाई खतरामा पार्न सक्छ।

अनलाइन निगरानीबाट मेटाडाटा सुरक्षित गर्ने उपायहरू

डिजिटल फाइल, सञ्चार र अनलाइन गतिविधिसँग सम्बन्धित मेटाडाटा अनजानमा नै तेस्रो पक्ष, प्लेटफर्म वा निगरानी संयन्त्रको पहुँचमा पर्न सक्छ। त्यसैले मेटाडाटाको दुरुपयोग रोक्न र डिजिटल गोपनीयता सुरक्षित गर्न निम्न उपायहरू अवलम्बन गर्नु आवश्यक हुन्छ।

- वेब ब्राउजरमा तेस्रो पक्ष (Third-party) कुकी तथा ट्र्याकिङ फिङ्गरप्रिन्टिङ सुविधा बन्द गर्ने, र सम्भव भएसम्म गोपनीयता मैत्री ब्राउजरहरू जस्तै TOR Browser, Firefox Browser तथा Incognito सेटिङहरूको प्रयोग गर्नुहोस्।

- इन्टरनेट प्रयोग गर्दा र त्यसमा पनि विशेष गरी सार्वजनिक वा असुरक्षित नेटवर्क प्रयोग गर्दा Virtual Private Network (VPN) प्रयोग गरी IP ठेगाना र लोकेसनसम्बन्धी मेटाडाटा सुरक्षित गर्नुहोस् ।

- एउटै ब्राउजरमा सबै गतिविधि नगरी, फरक–फरक कार्यका लागि फरक–फरक ब्राउजर प्रयोग गर्नुहोस्, जसले एकै ठाउँमा मेटाडाटा जम्मा हुनबाट रोक्छ ।

- Word, Excel, PDF जस्ता फाइलहरूमा प्रायः लेखकको नाम (Author's Name), संस्थाको विवरण (Organization), संशोधन इतिहास (Revision History), टिप्पणीहरू (Comments) लगायतका मेटाडाटा स्वतः रेकर्ड हुने गर्छन् । यस्ता मेटाडाटाले फाइल साझा गर्दा पत्रकारको पहिचान, संस्थागत सम्बन्ध वा कार्यप्रक्रियाहरुको बारेमा थाहा हुन सक्छ । त्यसैले कुनै फाइल बेनामी रूपमा (anonymously) वा संवेदनशील सन्दर्भमा साझा गर्नु अघि Document Properties / Metadata हटाउने (Inspect Document, Remove Metadata) प्रक्रिया अनिवार्य रूपमा अपनाउनुहोस् ।

- फोटो, भिडियो वा कागजात पठाउनु अघि मेटाडाटा हटाउने उपकरणहरू (जस्तै: ExifCleaner, Scrambled EXIF) प्रयोग गरी अनावश्यक विवरण हटाउनुहोस् ।

- मेसेजिङ एपहरूमा 'पढिएको सूचना' (Read Receipt) र 'टाइप गरिरहेको देखाउने सङ्केत' (Typing Indicator) जस्ता सुविधाहरू बन्द गर्नुहोस्, ताकि सञ्चारको समय, व्यवहार र गतिविधिसम्बन्धी मेटाडाटा न्यूनतम रहोस् ।

- संवेदनशील फाइलहरू सुरक्षित फोल्डर वा पासवर्डले सुरक्षित गरिएको सङ्ग्रह (जस्तै: 7Zip, VeraCrypt) भित्र राखी मात्र भण्डारण वा आदान–प्रदान गर्नुहोस् ।

- क्लाउडमा फाइल अपलोड गर्दा End-to-End Encryption उपलब्ध गराउने सुरक्षित प्लेटफर्म (जस्तै: Proton Drive) प्रयोग गर्नुहोस् । सामान्य रूपमा प्रयोग हुने Google Drive वा Dropbox जस्ता सेवाहरू संवेदनशील सामग्रीका लागि प्रायः पर्याप्त सुरक्षित नहुन सक्छन् ।
- क्लाउड सेवा प्रयोग गर्दा minimum safe configuration का आधारभूत सुरक्षा अभ्यासहरू अनिवार्य रुपमा पालना गर्नुहोस् ।
- RAW फाइल, original footage वा असम्पादित सामग्री सिधै व्यक्तिहरूलाई साझा गर्दा दुरुपयोगको जोखिम रहने भएकाले, आवश्यक सम्पादन, ब्लर, वा redaction (संवेदनशिल सूचनालाई नदेखिने बनाउने) गरेपछि मात्र साझा गर्नुहोस् ।

२.४ सुरक्षित इन्टरनेट प्रयोग

पत्रकारका लागि सुरक्षित इन्टरनेट प्रयोग र विश्वसनीय एप तथा सफ्टवेयरको प्रयोग अत्यन्त महत्त्वपूर्ण हुन्छ, किनकि यसले स्रोतको गोपनीयता, समाचार सामग्रीको सुरक्षा र व्यक्तिगत डाटाको संरक्षण सुनिश्चित गर्छ। असुरक्षित ब्राउजर वा अनधिकृत सफ्टवेयरको प्रयोगले ह्याकिङ, डाटा चोरी र निगरानीको जोखिम बढाई पत्रकारिताको स्वतन्त्र र जिम्मेवार अभ्यासमा असर पार्न सक्छ ।

२.४.१ सुरक्षित ब्राउजिङ्ग:

क) अद्यावधिक सञ्चालन प्रणाली र ब्राउजरको प्रयोग: आफ्नो वेब ब्राउजर (जस्तै Chrome, Firefox, Safari) तथा सञ्चालन प्रणाली (अपरेटिङ सिस्टम-OS) लाई सधैँ नवीनतम संस्करणमा अद्यावधिक गरेर राख्नुपर्छ। नियमित अद्यावधिकले सुरक्षा कमजोरीहरू सुधार गरी अनलाइन जोखिमबाट जोगिन मद्दत गर्छ ।

ख) VPN प्रयोग: VPN (Virtual Private Network) ले इन्टरनेट

ट्राफिकलाई इन्क्रिप्ट गरी सुरक्षित माध्यमबाट प्रवाह गराउँछ । यसले प्रयोगकर्ताको लोकेशन, ब्राउजिङ गतिविधि र अनलाइन पहिचान लाई बाह्य निगरानी, ट्र्याकिङ तथा सार्वजनिक Wi-Fi बाट हुने सम्भावित जोखिमबाट जोगाउँछ । साथै, VPN ले प्रतिबन्धित वा ब्लक गरिएका वेबसाइटहरूमा सुरक्षित पहुँच दिन सक्छ । तर VPN प्रयोग गर्दा पूर्ण रुपमा anonymity सुनिश्चित गर्छ भन्ने भ्रममा पर्नु हुँदैन किनकि VPN साइबरसुरक्षाको एक उपाय हो, अदृश्य बनाउने साधन होइन । विशेषगरी निःशुल्क (free) VPN सेवाहरूले प्रयोगकर्ताको डाटा सङ्कलन वा तेस्रो पक्षलाई बिक्री गर्ने जोखिम रहन्छ । त्यसैले VPN प्रयोग गर्दा विश्वसनीय, प्रयोगकर्ताको जानकारी सङ्ग्रह नगर्ने नीति रहेका (no-log policy) पालना गर्ने र उच्च सुरक्षा मापदण्ड भएका सेवा प्रदायक मात्र प्रयोग गर्नु उपयुक्त हुन्छ । साथै, अत्यन्त संवेदनशील काम गर्दा सार्वजनिक Wi-Fi को सट्टा व्यक्तिगत मोबाइल हटस्पट (personal hotspot) प्रयोग गर्नु अझ सुरक्षित अभ्यास मानिन्छ, किनकि यसले नेटवर्कमा आधारित आक्रमणको जोखिमलाई उल्लेखनीय रूपमा कम गर्छ ।

ग) **फिसिङप्रतिको सावधानी:** शङ्कास्पद लिङ्क, इमेल वा सन्देशमा आएका लगइन अनुरोधमा क्लिक नगर्नुहोस् । सो वेबसाइट प्रयोग गर्न आवश्यक भएमा उक्त लिङ्क प्रयोग नगरी आधिकारिक वेबसाइटमा सिधै गएर लगइन गर्ने बानी बसाल्नुपर्छ ।

घ) **TOR ब्राउजर:** उच्च जोखिमयुक्त अनुसन्धान, संवेदनशील विषयको खोज, वा निगरानीको सम्भावना भएका अवस्थामा TOR browser प्रयोग गर्न सकिन्छ । Tor ले ट्राफिकलाई धेरै तहमा इन्क्रिप्ट गरी पठाउने भएकाले पहिचान, लोकेशन र ब्राउजिङ गतिविधि गोप्य राख्न सहयोग गर्छ । तर TOR ब्राउजर सामान्य दैनिक ब्राउजिङका लागि नभई विशेष जोखिम अवस्थाहरूमा मात्र सावधानीपूर्वक प्रयोग गर्नु उपयुक्त हुन्छ ।

२.४.२ सुरक्षित एप/सफ्टवेयर प्रयोग

क आधिकारिक डाउनलोड: एपहरू सधैँ आधिकारिक एप स्टोर (App Store/Play Store) वा निर्माताको वेबसाइटबाट मात्र डाउनलोड गर्नुहोस्। तेस्रो पक्ष (Third-Party) स्रोतबाट कहिल्यै एपहरू इन्स्टल नगर्नुहोस्।

ख) अनुमति जाँच: कुनै पनि नयाँ एप इन्स्टल गर्दा त्यसले मागेको अनुमतिहरू (Permissions) (जस्तै: क्यामेरा, माइक्रोफोन, लोकेसन, सम्पर्क सूचीमा दिइएको पहुँच) को सावधानीपूर्वक समीक्षा गर्नुहोस्। उदाहरणका लागि, "एक साधारण टर्चलाइट एपलाई माइक्रोफोनको अनुमति किन चाहिन्छ" भन्ने प्रश्न आफैलाई सोध्नुहोस्।

ग) सुरक्षित संवाद: स्रोतहरूसँग संवेदनशील कुराकानी गर्नका लागि एन्ड-टू-एन्ड इन्क्रिप्टेड मेसेन्जर (जस्तै Signal) को प्रयोग गर्नुहोस्।

२.५ अनलाइन आक्रमण तथा लक्षित हमलाको सम्बोधन

अनलाइन उत्पीडन (Online Attacks) लाई बेवास्ता गर्नु वा त्यसको सामना गर्न तयार नहुनु दुवै जोखिमपूर्ण हुन्छ। यस खण्डले अनलाइन आक्रमण वा लक्षित हमलालाई चिन्न, त्यसको प्रभावलाई कम गर्न र आधिकारिक निकायमा रिपोर्ट गर्नका लागि मार्गदर्शन प्रदान गर्दछ।

२.५.१ लिङ्गमा आधारित वा राजनीतिक उत्पीडन पहिचान

लिङ्गमा आधारित उत्पीडन प्रायः महिला तथा सीमान्तकृत समुदायका पत्रकारहरूलाई लक्षित गरी उनीहरूको पेसागत विश्वसनीयतामाथि प्रहार गर्ने उद्देश्यले प्रयोग गरिन्छ। यस्ता आक्रमणहरू पहिचान गर्न निम्न पक्षहरूलाई ध्यानपूर्वक अवलोकन र विचार गर्न सकिन्छ:

- शरीर, पहिरन वा व्यक्तिगत सम्बन्धसम्बन्धी अपमानजनक टिप्पणीहरू।

- यौनजन्य तस्बिर वा सन्देश (Sexting / Unsolicited Nudes) पठाउने कार्य।
- परिवारका सदस्यहरूलाई धम्की दिने प्रवृत्ति (विशेषगरी महिला पत्रकारका बालबालिका वा परिवारलाई लक्षित गर्दै)।
- चरित्र हत्या गर्ने वा 'स्लट शेमिङ' (Slut-Shaming) जस्ता अपमानजनक अभियान सञ्चालन गर्ने प्रयास।

त्यस्तै राजनीतिक रूपमा लक्षित आक्रमणहरू प्रायः कुनै संवेदनशील वा अनुसन्धानात्मक रिपोर्टिङ पश्चात् राजनीतिक दल, कर्पोरेट स्वार्थ समूह वा अन्य सङ्गठित समूहहरूबाट सुरु हुने गरेको पाइन्छ।

- **डक्सिङ (Doxing):** कुनै व्यक्तिको निजी विवरणहरू, जस्तै घरको ठेगाना, फोन नम्बर वा अन्य व्यक्तिगत जानकारी, अनुमति बिना सार्वजनिक रूपमा फैलाउने कार्य।
- **डगपाइलिंग (Dogpiling):** एउटै सन्देश, पोस्ट वा व्यक्तिलाई लक्षित गरी सयौँ वा हजारौँ नक्कली, स्वचालित वा सङ्गठित खाताहरूबाट एकैचोटि आक्रमण वा दुर्व्यवहार गर्ने कार्य।
- **प्रतिलिपि अधिकार दुरुपयोग (Copyright Abuse):** सामग्री हटाउन दबाब सिर्जना गर्न गलत कपीराइट दाबी गर्ने अभ्यास।
- **फिशिङ (Phishing):** नक्कली इमेल, सन्देश वा वेबसाइट प्रयोग गरी खाता, पासवर्ड वा संवेदनशील जानकारी ह्याक गर्न खोज्ने कार्य।
- **स्लट–शेमिङ (Slut-Shaming):** विशेषगरी महिला वा लैङ्गिक रूपमा सीमान्तकृत व्यक्तिलाई उनको पहिरन, व्यवहार, व्यक्तिगत सम्बन्ध वा यौनिकतासँग जोडेर अपमानित गर्ने, बदनाम गर्ने वा चरित्र हत्या गर्ने अभ्यास।

२.५.२ उत्पीडन कम गर्ने व्यावहारिक उपायहरू

अनलाइन प्लेटफर्ममार्फत हुने आक्रमणको सामना गर्दा के गर्ने भन्ने प्रश्न डिजिटल सुरक्षा सुनिश्चितताको एक प्रमुख र व्यावहारिक विषय हो । यस्तो उत्पीडनको सामना गर्नुपरेमा त्यसबाट हुने सम्भावित क्षति र मानसिक तनाव कम गर्नका लागि निम्न उपायहरू तत्काल अपनाउनु आवश्यक हुन्छ:

- **प्रमाण सङ्कलन:** धम्कीपूर्ण सन्देश, पोस्ट तथा प्रतिक्रियाहरूलाई मिति र समय स्पष्ट देखिने गरी स्क्रिनसट लिने वा रेकर्डिङ गरी सुरक्षित राख्नुहोस् ।
- **अनलाइन उपस्थिति सीमित गर्ने:** सामाजिक सञ्जालमा पोस्ट वा ट्वीटमा कमेन्ट गर्न सक्ने सुविधा सीमित गरी तपाईले उल्लेख गरेका व्यक्ति मात्र वा Friends only मा सेट गर्ने, वा आवश्यक परे कमेन्ट सुविधा अस्थायी रूपमा बन्द गर्नुहोस् ।
- **ब्लक र म्युट गर्ने:** निरन्तर उत्पीडन गर्ने वा आक्रमणमा संलग्न खाताहरूलाई आवश्यकता अनुसार ब्लक वा म्युट गर्नुहोस् ।
- **सहकर्मी वा विश्वासिलो व्यक्तिलाई जानकारी दिने:** सम्पादक, विश्वासिलो सहकर्मी वा सम्बन्धित सुरक्षा निकायलाई घटनाबारे जानकारी गराउने र आवश्यक भएमा मानसिक स्वास्थ्य सहयोग (Mental Health Support) लिनुहोस् ।
- **पासवर्ड र सुरक्षा सेटिङ अद्यावधिक गर्ने:** कुनै पनि रूपमा खाता ह्याक भएको शङ्का लागेमा तुरुन्तै सबै महत्त्वपूर्ण खाताहरूको पासवर्ड परिवर्तन गर्ने र बहु-कारक प्रमाणीकरण (MFA) सक्रिय गरिएको सुनिश्चित गर्नुहोस् ।

२.५.३ अनलाइन आक्रमण वा लक्षित हमलाको अवस्थामा प्रतिक्रिया (Incident Response)

क) तत्काल गर्ने कार्य (Immediate Actions)

- खाता सुरक्षित गर्न पासवर्ड परिवर्तन गर्नुहोस्।
- सम्भव भएमा 2FA/MFA पुनः सक्रिय वा reset गर्नुहोस्।
- शङ्कास्पद लगइन सेसन/डिभाइस revoke गर्नुहोस्।
- संवेदनशील काम अस्थायी रूपमा रोक्नुहोस्।

ख) छोटो अवधिमा गर्ने सकिने कार्य (Short-term Actions)

- सम्बन्धित प्लेटफर्ममा Incident रिपोर्ट गर्नुहोस्।
- Recovery इमेल, फोन नम्बर जाँच गर्नुहोस्।
- सम्भावित secondary compromise (email, social media) को मूल्याङ्कन गर्नुहोस्।
- आफूसम्बन्धित संस्थामा तत्काल supervisor/editor/management लाई जानकारी गराउनुहोस्।
- गम्भीर जोखिम वा धम्कीको अवस्थामा साइबर ब्युरो, कानुनी निकाय वा प्रहरीमा उजुरी गर्नुहोस्।
- घटनासँग सम्बन्धित डिजिटल प्रमाण सुरक्षित राख्नुहोस्।

२.५.४ प्लेटफर्म वा सम्बन्धित निकायमा रिपोर्ट गर्ने प्रक्रिया

क) प्लेटफर्महरुमा रिपोर्ट गर्ने प्रक्रिया

सबै प्लेटफर्महरूमा 'उत्पीडन' र 'घृणास्पद अभिव्यक्ति' विरुद्ध रिपोर्टिङ गर्नका लागि व्यवस्थाहरू उपलब्ध हुन्छन्। उदाहरणका लागि:

Facebook मा रिपोर्ट गर्ने तरिका:

- समस्याजनक पोस्ट वा फोटो खोल्नुहोस्।

- माथि देखिने तीन वटा डट (…) मा थिच्नुहोस्।
- "Report post/photo" मा थिच्नुहोस्।
- किन यो पोस्ट मिथ्या, भ्रामक वा समस्याजनक हो भन्ने कारण छान्नुहोस्।
- अन्त्यमा देखिएको विकल्पमा थिचेर **Submit** गर्नुहोस्।

ख) संस्थागत र कानुनी निकाय (Institutional and Legal Bodies)

यदि अनलाइन दुर्व्यवहार, धम्की वा डिजिटल आक्रमण गम्भीर प्रकृतिको छ भने केवल प्लेटफर्ममा रिपोर्ट गर्नु मात्र पर्याप्त नहुन सक्छ। यस्तो अवस्थामा आफू कार्यरत संस्थामा र कानुन कार्यान्वयन निकायमा पनि जानकारी दिनु आवश्यक हुन्छ।

- **कार्यरत निकाय:** सबैभन्दा पहिले आफू आबद्ध सञ्चार गृहका सम्पादक वा मानव संसाधन (HR) विभागलाई घटनाबारे औपचारिक रूपमा जानकारी गराउनुपर्छ। यसले संस्थागत सहयोग, सुरक्षा व्यवस्था र आवश्यक निर्णय लिन सहयोग गर्छ।

- **पत्रकार महासङ्घ वा नागरिक समाज:** यस्ता घटनाका सम्बन्धमा नेपाल पत्रकार महासङ्घ तथा डिजिटल सुरक्षा र अभिव्यक्ति स्वतन्त्रतामा काम गर्ने नागरिक समाज संस्थाहरू समक्ष पनि रिपोर्ट गर्न सकिन्छ। यी संस्थाहरूले कानुनी सल्लाह, दस्तावेजीकरण र आवश्यक अवस्थामा कानुनी प्रक्रियामा सहयोग उपलब्ध गराउन सक्छन्।

- **प्रहरी वा कानुनी निकाय:** यदि उक्त उत्पीडनको घटना गम्भीर धम्की, हिंसा वा कानुनी उल्लङ्घनसँग सम्बन्धित छ भने त्यस सम्बन्धमा प्रहरी वा कानुनी निकायमा प्रमाणसहित उजुरी दिनुपर्छ।

परिच्छेद ३

निर्वाचन, सूचना अखण्डता र तथ्यजाँच

३.१ निर्वाचनमा सूचना अखण्डताको महत्त्व

लोकतान्त्रिक निर्वाचनको विश्वसनीयता, निष्पक्षता र वैधता सुनिश्चित गर्न सूचना अखण्डता (Information Integrity) एक आधारभूत सर्त हो। मतदाताले सही, सन्तुलित र समयमै प्राप्त गरेको सूचनाका आधारमा विवेकपूर्ण निर्णय लिन सक्ने वातावरण निर्माण गर्नु नै सूचना अखण्डताको मुख्य उद्देश्य हो। डिजिटल प्लेटफर्म र सामाजिक सञ्जालको व्यापक प्रयोगसँगै निर्वाचन सम्बन्धी सूचनाको प्रवाह तीव्र, बहुआयामिक र प्रभावशाली बनेको छ, जसले सूचना अखण्डताका अवसरसँगै गम्भीर चुनौतीहरू पनि सिर्जना गरेको छ।

निर्वाचनको समयमा फैलिने मिथ्या सूचना (Misinformation), योजनाबद्ध भ्रामक सूचना (Disinformation) र कूसूचना (Malinformation) द्वारा सिर्जित सूचना अव्यवस्था (Information Disorder) ले मतदातालाई भ्रमित पार्ने, राजनीतिक ध्रुवीकरण बढाउने, सार्वजनिक विश्वास कमजोर बनाउने तथा निर्वाचन प्रक्रियाप्रति अविश्वास सिर्जना गर्ने जोखिम उत्पन्न गर्छ। यस्ता सूचनाले मतदाताको सहभागिता, उम्मेदवारको छवि, निर्वाचन निकायको विश्वसनीयता र अन्ततः लोकतान्त्रिक परिणाममाथि नै असर पार्न सक्छ।

डिजिटल प्रविधिको दुरुपयोगमार्फत् निर्वाचनसँग सम्बन्धित सूचनालाई अझ विश्वसनीय देखिने तर भ्रामक रूपमा प्रस्तुत गर्ने नयाँ-नयाँ रणनीतिहरू पनि देखिन थालेका छन्। जस्तै, नक्कली स्क्रिनसट (Fake Screenshots) तयार गरी विभिन्न व्यक्तिहरू बीचको संवाद वा कुनै सरकारी/गैरसरकारी निर्णयलाई गलत सन्दर्भमा प्रस्तुत गर्नु, आर्टिफिसिएल इन्टेलिजेन्स (एआई) प्रयोग गरी उम्मेदवार, पत्रकार वा निर्वाचन अधिकारीको आवाज वा भिडियो प्रयोग गरी भ्रामक सामग्री बनाउने (AI-Generated Audio/Video Impersonation), तथा पत्र, मेमो, सम्झौता वा अन्य कागजातमा मिति, लिखित विषयहरू वा शब्दहरू सानो मात्रामा परिवर्तन गरी "लिक" गरिएको जस्तो देखाउने (Manipulated Leaks) अभ्यासहरू समावेश छन् । यस्ता सामग्री प्रकाशित भइसकेपछि वास्तविक (original) कागजात सार्वजनिक गरी पत्रकारमाथि गलत सूचना फैलाएको आरोप लगाइने जोखिम समेत रहन्छ, जसले पत्रकारको पेसागत विश्वसनीयता र सार्वजनिक विश्वासमा गम्भीर क्षति पुर्‍याउन सक्छ।

यस सन्दर्भमा पत्रकारहरूको भूमिका अत्यन्त महत्त्वपूर्ण र जिम्मेवारपूर्ण हुन्छ । पत्रकारले सूचना सत्यापन, सन्दर्भको स्पष्टता, स्रोतको विश्वसनीयता र प्रस्तुतीकरणको सन्तुलनमा विशेष ध्यान दिँदै गलत, अपुरो वा भ्रामक सूचनाको पुनः प्रसार रोक्नुपर्छ। साथै, तथ्यमा आधारित, जिम्मेवार र नैतिक पत्रकारितामार्फत मतदातालाई सशक्त बनाउनु, सूचना अव्यवस्थाको पहिचान गर्नु र त्यसबारे सार्वजनिक सचेतना बढाउनु पत्रकारिताको केन्द्रीय दायित्व हो। सूचना अखण्डता कायम राख्नु केवल प्राविधिक अभ्यास नभई स्वतन्त्र, निष्पक्ष र विश्वसनीय निर्वाचन सुनिश्चित गर्ने लोकतान्त्रिक प्रतिबद्धता पनि हो।

मिथ्या सूचना (Misinformation)	भ्रामक सूचना (Disinformation)	कूसूचना (Malinformation)
मिथ्या सूचना हानि पुर्‍याउने नियतले तयार पारिएको भने हुँदैन। यो त्रुटिपूर्ण, अपूर्ण वा प्रसङ्ग हटाएर प्रस्तुत गरिएको जानकारी हुनसक्छ।	भाम्रक सूचना जानीजानी कुनै व्यक्ति, समूह, संस्था वा समुदायलाई हानी पुर्‍याउनका लागि तयार गरिएको हुन्छ। यो जानाजानी फैलाइएको झुट हो।	यो यथार्थमा आधारित सूचना हो, तर कुनै व्यक्ति, संस्था वा समुदायलाई हानी पुर्‍याउने उद्देश्यले प्रयोग गरिन्छ। यसमा गोप्य जानकारीलाई सार्वजनिक गर्ने जस्ता कार्यहरू पर्दछन्। यो सूचना आफैँमा सत्य भए पनि त्यसलाई गलत सन्दर्भ, समय वा उद्देश्यका साथ सार्वजनिक गरिन्छ।

३.२ तथ्यजाँच (Fact Check)

तथ्यजाँच (Fact-check) भनेको सार्वजनिक रूपमा प्रवाहित सूचना, दाबी, वक्तव्य वा सामग्रीको सत्यता, सन्दर्भ र प्रमाणका आधारमा व्यवस्थित रूपमा परीक्षण गर्ने प्रक्रिया हो। निर्वाचन जस्ता संवेदनशील समयमा तथ्यजाँचले गलत, अपुरो वा भ्रामक सूचनाको पहिचान गरी त्यसको प्रभाव न्यूनीकरण गर्न मद्दत गर्छ, जसले मतदाताको सूचित निर्णय, सार्वजनिक विश्वास र निर्वाचन प्रक्रियाको अखण्डता कायम राख्न योगदान पुर्‍याउँछ।

व्यवस्थित तथ्यजाँच प्रक्रिया प्रायः विशेष फ्याक्ट-चेक संस्थाहरूले अपनाउने अभ्यास भएता पनि पत्रकारितामा तथ्यजाँच छुट्टै तर अनिवार्य दायित्वका रूपमा रहन्छ। पत्रकारले समाचार प्रकाशन अघि स्रोतको विश्वसनीयता, दाबीको सन्दर्भ, तथ्यको पुष्टि र प्रमाणको पर्याप्तता सुनिश्चित गर्नुपर्छ। यसले पत्रकारितालाई भ्रामक

सूचनाको पुनः प्रसारबाट जोगाउनुका साथै समाचारको विश्वसनीयता र पेसागत आचारसंहिता कायम राख्न मद्दत गर्छ।

तथ्यजाँचका प्रमुख पाटोहरूमा स्रोत परीक्षण, सन्दर्भ (context) को विश्लेषण, मिति र स्थानको पुष्टि, फोटो तथा भिडियो सामग्रीको प्रामाणिकता जाँच (जस्तै रिभर्स सर्च), र अन्य विश्वसनीय माध्यम वा आधिकारिक अभिलेखसँग तुलना गर्ने प्रक्रिया समावेश हुन्छन्। पत्रकारका लागि तथ्यजाँच केवल एउटा प्राविधिक चरण मात्र नभई, जिम्मेवार, नैतिक र जनहितमुखी पत्रकारिताको आधारशिला हो, जसले सूचना अखण्डता र लोकतान्त्रिक अभ्यासलाई सुदृढ बनाउँछ।

३.३ तथ्य जाँचमा प्रविधिको प्रयोग

सामाजिक सञ्जाल र इन्टरनेटको व्यापक प्रयोगले कुनै पनि सूचना क्षणभरमै ठुलो जनसमुदायसम्म फैलिन सक्ने अवस्था सिर्जना गरेको छ, जसका कारण कुनै सामग्री भाइरल हुन धेरै समय लाग्दैन । तर कुनै सामग्री भाइरल हुनु स्वयं त्यसको विश्वसनीयता वा सत्यताको प्रमाण हुँदैन । विशेषगरी निर्वाचन, आन्दोलन, राजनीतिक अस्थिरता वा अन्य संवेदनशील घटनाका समयमा हेरफेर गरिएका, मिथ्या तथा भ्रामक सूचनाहरूलाई जानाजानी व्यापक रूपमा फैलाउने प्रवृत्ति बढ्ने गरेको देखिन्छ। त्यसैले पत्रकार तथा मिडियाकर्मीहरूले भाइरल सामग्रीमा देखिन सक्ने केही सामान्य चेतावनीका सङ्केतहरू (red flags) पहिचान गर्न सक्ने क्षमता विकास गर्नु आवश्यक हुन्छ।

३.३.१ फोटो, भिडियो, सामाजिक सञ्जाल पोस्ट र दाबी छिटो प्रमाणीकरण गर्ने तरिका

सामाजिक सञ्जालले सूचनाको सम्प्रेषण र प्रवाहको स्वरूपमा गहिरो परिवर्तन ल्याएको छ। सामाजिक सञ्जालमा प्रवाह हुने फोटो, भिडियो तथा पोस्टहरूमा केवल तस्बिर वा भिडियोमा गरिएको परिवर्तन, एआईको प्रयोग मात्र होइन, तिनसँग जोडिएका क्याप्सन, शीर्षक वा सन्देशमार्फत पनि अफवाह, मिथ्या वा भ्रामक

समाचार फैलाइने सम्भावना रहन्छ । त्यसैले यस्ता फोटो, भिडियो तथा सामाजिक सञ्जाल पोस्टहरूको प्रमाणीकरण गर्नु अत्यन्त आवश्यक हुन्छ । यस्ता सामग्रीको प्रमाणीकरण गर्ने केही प्रमुख तरिकाहरू निम्नानुसार रहेका छन्:

क) आफूलाई प्रश्न गर्ने

कुनै फोटो वा भिडियो हेर्दा त्यसलाई तुरुन्तै सत्य मान्नु अघि आफैलाई केही आधारभूत प्रश्नहरू सोध्नुपर्छ, जस्तै:

- यो सामग्री कसले पोस्ट गरेको हो ?
- यो सामग्री कहिले पोस्ट गरिएको हो ? (के पुरानो सामग्रीलाई "आज" भनेर पुनः फैलाइएको हो ?)
- यो सामग्री अहिले किन फैलिएको छ ? (Why now ?)
- के यो कुनै घटना वा विवादसँग जोडिएको सङ्गठित रूपमा फैलाइएको सामग्री (coordinated push) हो ?
- भिडियोमा कुन भाषा बोलिएको छ र त्यो सन्दर्भसँग मेल खान्छ कि खाँदैन ?
- "के साँच्चै यस्तो हो ?", "लुकाइएको सत्य के हो ?" जस्ता षड्यन्त्रात्मक (conspiracy) भाव झल्किने भाषा प्रयोग गरिएको छ कि छैन ?
- शीर्षक वा क्याप्सन तथ्यमा आधारित छ कि अत्यधिक भावनात्मक वा उत्तेजनात्मक शब्दावली प्रयोग गरिएको छ ?

ख) फोटो वा भिडियोमा चलखेल गरिएको छ कि छैन भनेर विश्लेषण गर्ने

फोटो वा भिडियोको प्रामाणिकता मूल्याङ्कन गर्दा त्यसमा कुनै प्रकारको छेडछाड, सम्पादन वा कृत्रिम रूपमा सिर्जना गरिएको सङ्केत देखिन्छ कि छैन भन्ने कुरा ध्यानपूर्वक विश्लेषण गर्नुपर्छ । यसका लागि निम्न पक्षहरू जाँच गर्न सकिन्छ:

- छाया र प्रकाश (shadow and lighting) स्वाभाविक देखिन्छ कि देखिँदैन भन्ने कुरा अवलोकन गर्नुहोस्।
- कृत्रिम बुद्धिमत्ता (AI) प्रयोग भएको सङ्केत छ कि छैन भन्ने पहिचान गर्न अस्वाभाविक आँखा झिम्क्याएको, दाँत वा औँलाहरू अस्वाभाविक देखिएको, अनुहार वा पृष्ठभूमिहरू दोहोरिएको (repeating patterns) जस्ता सङ्केतहरू जाँच गर्नुहोस्।
- आवश्यक परे Hive Moderation, Sensity AI Detect, Deepfakes DeepBrain AI, AccuL, Google SynthID जस्ता उपकरणको सहायताबाट प्रारम्भिक विश्लेषण गर्नुहोस्।
- आवाज र दृश्यबीच तालमेल (audio-video match) छ कि छैन जाँच गर्नुहोस्।
- कपडाको बनावट, घरको आकार, बाटोको संरचना, होर्डिङ बोर्ड वा अन्य भौतिक विवरणहरूले स्थान वा समयबारे केही सङ्केत दिन्छन् कि छैनन् भन्ने कुरा विश्लेषण गर्नुहोस्।
- बिजुलीका पोल, साइनबोर्ड, सवारी साधनका नम्बर प्लेट जस्ता सङ्केतहरूलाई ध्यानपूर्वक अवलोकन गर्नुहोस्।
- पुराना फोटो वा भिडियोहरूलाई नयाँ समाचारको सन्दर्भसँग जोडेर पुनः प्रयोग गरिएको छ कि छैन भन्ने कुरा जाँच गर्नुहोस्।

कुनै सामग्री एल्गोरिदम र एआई प्रयोग गरेर बनाइने नक्कली वा भ्रामक छ कि छैन भनेर जाँच्नका लागि डीपफेक एनालाइसिस युनिट (DAU) सँग समेत समन्वय गर्न सकिन्छ।

डीपफेक एनालाइसिस युनिट (DAU)

डीपफेक एनालाइसिस युनिट (DAU) भनेको मिसइनफर्मेसन कम्ब्याट एलायन्स (Misinformation Combat Alliance-MCA) अन्तर्गत सञ्चालित एक विशेष इकाई हो । यसको मुख्य उद्देश्य एल्गोरिदम र एआई प्रयोग गरेर बनाइने नक्कली वा भ्रामक मिडिया (जस्तै: डीपफेक भिडियो, अडियो, तस्बिर) को पहिचान, विश्लेषण र नियन्त्रणमार्फत जनचेतना बढाउनु हो । DAU ले प्रयोगकर्ताहरूलाई WhatsApp हेल्पलाइन मार्फत शङ्कास्पद वा भ्रामक सामग्री रिपोर्ट गर्ने व्यवस्था गरेको छ । यसरी रिपोर्ट गरिएका सामग्रीहरूलाई फ्याक्ट चेकिङ संस्थाहरू सँग समन्वय गरी जाँच, मूल्याङ्कन र प्रमाणीकरण गरिन्छ ।

पत्रकारहरूले DAU को WhatsApp हेल्पलाइनमार्फत शङ्कास्पद सामग्री रिपोर्ट गर्न सक्छन् भने त्यसरी रिपोर्ट गरिएको सामग्रीको विभिन्न फ्याक्ट चेकिङ संस्थाहरूबाट हुने विश्लेषणका आधारमा डीपफेक र एआई आधारित मिथ्या वा भ्रामक सूचना पहिचान गर्दै मिथ्या वा भ्रामक सूचना प्रकाशनको जोखिम घटाउन, समाचारको विश्वसनीयता बढाउन र तथ्यमा आधारित, जिम्मेवार पत्रकारिता गर्न फाइदा लिन सक्छन् ।

ग) रिभर्स इमेज/भिडियो खोज (Reverse Image/Video Search)

तस्बिर वा भिडियो प्रयोग गर्नु अघि रिभर्स इमेज वा भिडियो खोज (Reverse Image/Video Search) एक उपयोगी अभ्यास हो । यस प्रक्रियाले उक्त तस्बिर वा भिडियो पहिले कहिले र कहाँ प्रयोग गरिएको थियो भन्ने जानकारी पाउन मद्दत गर्छ । साथै, कुनै पुरानो घटना, फरक देश वा फरक सन्दर्भसँग सम्बन्धित सामग्रीलाई नयाँ घटनासँग जोडेर पुनः प्रयोग गरिएको त होइन भन्ने कुरा पनि स्पष्ट गर्न सकिन्छ । यसका लागि फोटो सिधै रिभर्स इमेज सर्चमार्फत जाँच गर्न सकिन्छ भने भिडियोको हकमा प्रारम्भिक ५-१० सेकेन्डको क्लिप वा उपयुक्त फ्रेम निकालेर रिभर्स सर्च गर्नु प्रभावकारी हुन्छ ।

ङ) प्रसारित दाबीको सन्दर्भ (Context) खोजी

प्रसारित दाबी कुन सन्दर्भ (context) मा गरिएको हो भनी उल्लेख नहुनु प्रायजसो अवस्थामा भ्रामक वा हेरफेर गरिएको सामग्री हुनसक्छ भन्ने महत्त्वपूर्ण सङ्केत हो । त्यसैले सामग्रीमा प्रस्तुत दाबी, समय, स्थान, व्यक्ति र परिस्थितिबारे प्रश्न गर्नु आवश्यक हुन्छ । यसका लागि सम्बन्धित किवर्ड प्रयोग गरी समाचार खोजी गर्नु, उक्त दाबी पछिल्ला वा विगतका घटनासँग मिल्दोजुल्दो छ कि छैन भनेर जाँच गर्नु, तथा सो सामग्री सही सन्दर्भमा प्रस्तुत गरिएको छ कि छैन भन्ने कुरा पुष्टि गर्नु तथ्यजाँच प्रक्रियाको महत्त्वपूर्ण पाटो हो ।

च) सामग्रीको स्रोत जाँच

विश्वसनीय सामग्रीमा प्रायः स्पष्ट स्रोत, मिति, स्थान वा आधिकारिक निकायको उल्लेख भएको हुन्छ । त्यसैले समाचार, रिपोर्ट वा सामाजिक सन्देश जाँच गर्दा स्रोतको विश्वसनीयतालाई प्राथमिकता दिएर हेर्नु आवश्यक हुन्छ । स्रोत नखुलेको वा अस्पष्ट सामग्री, जस्तै "विश्वस्त स्रोतका अनुसार", "सामाजिक सञ्जालमा भाइरल" भनी उल्लेख भएका सामग्रीप्रति विशेष रूपमा सतर्क रहनु पर्छ । स्रोतको प्रमाणिकता जाँच गर्नका लागि सम्बन्धित संस्थाको वेबसाइट, आधिकारिक प्रेस विज्ञप्ति वा प्रमाणित समाचार माध्यमबाट पुष्टि गर्ने अभ्यास अपनाउनुपर्छ । यसले तथ्यजाँचको विश्वसनीयता र पत्रकारिताको गुणस्तर सुनिश्चित गर्न मद्दत पुर्‍याउँछ ।

छ) सामाजिक सञ्जाल खाताको प्रमाणिकता जाँच

सामाजिक सञ्जालमा फैलिने सामग्रीको सत्यता सुनिश्चित गर्न पत्रकारहरूले खाता प्रमाणिकता जाँच गर्नु अत्यन्त महत्त्वपूर्ण हुन्छ । यसले पत्रकारलाई सामग्रीको स्रोत विश्वसनीय छ कि छैन भन्ने निर्धारण गर्न, भ्रामक वा पूर्वाग्रही सूचना पहिचान गर्न, र तथ्यजाँच प्रक्रियामा सही निर्णय लिन मद्दत गर्छ ।

- सामग्री साझा गर्ने सामाजिक सञ्जाल खाताले कहिले खोलिएको हो र पहिले कस्ता प्रकारका सामग्री पोस्ट गरिएका रहेछन् भन्ने समीक्षा गर्नुहोस् ।

- खाता नियमित रूपमा प्रमाणित स्रोत, आधिकारिक समाचार पृष्ठ वा तथ्यपूर्ण सामग्री मात्र साझा गर्दै आएको छ कि छैन जाँच गर्नुहोस्।
- कमेन्ट वा प्रतिक्रियाहरू एकै शैली वा एकै लाइनमा दोहोरिएका छन् कि छैनन् (coordinated messaging) भन्ने बारेमा ध्यान दिनुहोस्।
- उक्त सामाजिक सञ्जाल खाताले कुनै विशेष राजनीतिक दल, उम्मेदवार वा मुद्दालाई निरन्तर प्रवर्द्धन गर्दै आएको छ कि छैन हेर्नुहोस्।

नयाँ, शङ्कास्पद वा अत्यधिक राजनीतिक सामग्री पोस्ट गर्ने अकाउन्टबाट आएका सामग्रीप्रति विशेष सतर्कता अपनाउनु आवश्यक छ।

ज) अन्य मिडिया कभरेज जाँच (Other Media Coverage Check)

अन्त्यमा, कुनै दाबी वा घटनाबारे अन्य विश्वसनीय मिडिया संस्थाहरूले रिपोर्ट गरेका छन् कि छैनन् भन्ने कुरा जाँच गर्नु महत्त्वपूर्ण हुन्छ। त्यसैले उक्त विषयलाई कुनै राष्ट्रिय वा स्थानीय स्थापित मिडियाले समेटेका छन् कि छैनन् र आधिकारिक निकाय वा सरोकारवाला संस्थाबाट पुष्टि भएको छ कि छैन भन्ने जाँच गर्नुहोस् । यदि अन्य मिडियाले उक्त दाबी समेटेका छैनन् भने समाचारको रूपमा प्रस्तुत गर्नु अघि थप पुष्टि र अतिरिक्त सावधानी अपनाउनु जरूरी हुन्छ।

३.४ जिम्मेवार रिपोर्टिङ अभ्यास

१. मिथ्या वा भ्रामक जानकारीको प्रचार नगर्ने

- सामाजिक सञ्जालमा सामग्री पोस्ट गर्नु अघि त्यसको सत्यता र उपयुक्तता सुनिश्चित गर्नुहोस्। केवल प्रमाणित, विश्वसनीय र सान्दर्भिक जानकारी मात्र सार्वजनिक गर्नु उत्तम अभ्यास हो।
- कुनै विषय वा प्रश्नमा स्पष्ट र सही जानकारी प्रदान गर्दा, स्रोतहरू के जान्न चाहन्छन् भन्ने बारेमा ध्यान दिँदै प्रश्नहरूको प्रत्यक्ष, तथ्यमा आधारित उत्तर दिनुहोस्।

- अनलाइनमा धेरै प्रयोगकर्ताले सम्पूर्ण समाचार भन्दा शीर्षकलाई बढी हेर्छन्। त्यसैले शीर्षकले सामग्रीको सत्यता र उद्देश्यलाई स्पष्ट रूपमा प्रतिबिम्बित गर्ने र भ्रम सिर्जना नगर्ने सुनिश्चित गर्नुहोस् ।
- सामग्री तथ्य (fact) हो वा विचार/मत (opinion) हो भन्ने स्पष्ट छुट्टाउनुहोस्।
- जाँच नगरी सामग्री सेयर गर्दा उत्पन्न हुन सक्ने प्रभावबारे विचार गर्नुहोस्।

२. अफवाह रिपोर्ट गर्दा सावधानी अपनाउने

झुटा दाबीहरू पटक पटक दोहोरिएर प्रकाशन वा प्रसारण भइरहँदा मानिसहरूले त्यस्ता कुरा पत्याउन सक्ने भएकाले, अफवाह वा झुटो दाबी समाचारमा समावेश भएको देखिएमा त्यसलाई खारेज गरी सत्य जानकारी र प्रमाणमा आधारित कुरामा जोड दिनुहोस्। यसका साथै, आफ्नो रिपोर्टिङ प्रक्रिया र निर्णयहरूको पारदर्शिता दर्शक वा पाठकसमक्ष स्पष्ट रूपमा प्रस्तुत गर्नुहोस्, जसले समाचारको विश्वसनीयता र विश्वासलाई बलियो बनाउँछ।

३. तथ्यजाँच संस्थाहरू र न्युज रूम प्रमाणीकरण टिमसँग सहकार्य

शङ्का लाग्ने समाचार वा सूचना पुष्टि गर्न तथ्यजाँच (Fact-Checking) संस्थाहरू र न्युज रूम भित्रका प्रमाणीकरण (Verification) टिमसँग नियमित सहकार्य गर्नु अत्यन्त आवश्यक छ। यसरी सहकार्य गर्दा सामग्रीको सत्यता छिटो र विश्वसनीय रूपमा जाँच्न सकिन्छ र आवश्यक परे सम्बन्धित विशेषज्ञ वा प्रमाणित स्रोतको सहयोग लिन सकिन्छ। यस्तो अभ्यासले अफवाह र झूटो दाबीको जोखिम कम गर्ने मात्र होइन, पाठक र दर्शकसँगको विश्वासलाई पनि बलियो बनाउँछ, साथै पत्रकारिताको गुणस्तर र जिम्मेवारी सुनिश्चित गर्न मद्दत पुर्‍याउँछ।

३.५ द्रुत तथ्यजाँच चेकलिस्ट

स्रोत जाँच (Source Check)	• उक्त सामग्री कसले पोस्ट गरेको हो? • उक्त खाता वा स्रोत किन र कुन सन्दर्भमा अहिले भाइरल भइरहेको छ ?
सन्दर्भ जाँच (Context Check)	• सामग्री कहाँ र कहिले सिर्जना वा प्रकाशित गरिएको हो ? • हालको दाबी प्रस्तुत गरिएको सन्दर्भ सही र पूर्ण छ कि छैन ?
रिभर्स खोज (Reverse Search)	• प्रयोग गरिएको फोटो वा भिडियो पुरानो, पुनः प्रयोग गरिएको वा अन्य सन्दर्भको त होइन ? • सोही सामग्री पहिले अन्य घटनासँग जोडेर प्रयोग गरिएको थियो कि थिएन ?
डिजिटल चिन्ह/अवशेष जाँच (Artifact Check)	• फोटो वा भिडियोमा डिजिटल अवशेष (artifacts) देखिन्छन् कि छैनन् ? • आँखा, हात, दाँत, प्रकाश, छाया जस्ता तत्त्वहरू स्वाभाविक देखिन्छन् कि देखिदैनन् ?

अडियो जाँच (Audio Check)	• अडियोमा आवाज र ओठको चाल (lip movement) बीच सामञ्जस्यता छ कि छैन ? • आवाज कृत्रिम, सम्पादित वा AI-द्वारा सिर्जित भएको सङ्केत छ कि छैन ?
फ्रेम–फ्रेम जाँच (Frame-by-Frame Analysis)	• भिडियोको प्रत्येक फ्रेमलाई छुट्टाछुट्टै हेरी editing वा AI-जन्य हस्तक्षेपका सङ्केत छ कि छैन ?
खाताको इतिहास जाँच (Account History Check)	• खाता नयाँ, शङ्कास्पद वा असामान्य गतिविधि भएको त होइन ? • राजनीतिक उद्देश्यका लागि boosting वा coordinated activity गरिएको सङ्केत छ कि छैन ?
अन्य सञ्चारमाध्यमको रिपोर्टिङ (Other Media Coverage)	• सोही दाबी वा घटनालाई अन्य विश्वसनीय सञ्चारमाध्यमहरूले पनि रिपोर्ट गरेका छन् कि छैनन् ? • यदि गरेका छन् भने, विवरण र तथ्यहरू आपसमा मेल खान्छन् कि खाँदैनन् ?

परिच्छेद ४

डिजिटल युगमा निर्वाचन रिपोर्टिङ

डिजिटल प्रविधिको तीव्र विकाससँगै निर्वाचन प्रक्रिया र त्यससम्बन्धी सूचना प्रवाहको स्वरूप मौलिक रूपमा परिवर्तन भएको छ । सामाजिक सञ्जाल, अनलाइन समाचार पोर्टल, डिजिटल विज्ञापन र मोबाइल प्रविधिले गर्दा सूचनामा नागरिकको पहुँच सहज बनाएको छ । तर यसैसँगै मिथ्या वा भ्रामक सूचना, भ्रामक प्रचार, डिजिटल रूपान्तरण, घृणात्मक अभिव्यक्ति र गोपनीयता उल्लङ्घनजस्ता चुनौतीहरू पनि तीव्र रूपमा बढेका छन् । यस्तो डिजिटल वातावरणमा निर्वाचन रिपोर्टिङ केवल समाचार प्रकाशनको काम नभई लोकतान्त्रिक प्रक्रियाको विश्वसनीयता सुनिश्चित गर्ने महत्त्वपूर्ण जिम्मेवारी बनेको छ ।

विश्वसनीय पत्रकारिता स्वतन्त्र र निष्पक्ष निर्वाचनको आधार हो । नागरिकले आफ्नो मताधिकारको सही प्रयोग गर्न तथ्यमा आधारित, सन्तुलित र समयमै प्राप्त सूचना अपरिहार्य हुन्छ । डिजिटल प्लेटफर्ममार्फत फैलिने सूचनाले मतदाताको धारणा निर्माणमा प्रत्यक्ष प्रभाव पार्ने भएकाले, पत्रकारले प्रस्तुत गर्ने प्रत्येक समाचार, विश्लेषण र तथ्यजाँचले सार्वजनिक विश्वास निर्माण वा क्षय दुवै गर्न सक्छ । त्यसैले डिजिटल युगमा निर्वाचन रिपोर्टिङ गर्दा सत्यता, निष्पक्षता, पारदर्शिता र उत्तरदायित्वलाई केन्द्रमा राख्नु अनिवार्य हुन्छ ।

सूचनाको अधिकार लोकतान्त्रिक समाजको आधारभूत स्तम्भ हो । निर्वाचनमा उम्मेदवार चयनदेखि मतदान र परिणाम प्रकाशनसम्मको हरेक चरणका बारेमा

नागरिकलाई सही र प्रामाणिक जानकारी उपलब्ध गराउनु पत्रकारिताको मुख्य दायित्व हो। डिजिटल माध्यमले सूचनामा पहुँच विस्तार गरे पनि, मिथ्या, भ्रामक वा अपूर्ण सूचना प्रवाहले सूचनाको अधिकारलाई नै कमजोर बनाउन सक्छ। यस सन्दर्भमा पत्रकारले डिजिटल जोखिमहरू बुझ्दै, तथ्यजाँच, स्रोत प्रमाणीकरण, गोपनीयता संरक्षण र डिजिटल सुरक्षाका अभ्यास अपनाएर रिपोर्टिङ गर्नु अत्यन्त आवश्यक हुन्छ।

यस परिच्छेदले डिजिटल युगमा निर्वाचन रिपोर्टिङका अवसर र चुनौतीहरूलाई स्पष्ट गर्दै, पत्रकारलाई विश्वसनीय, सुरक्षित र अधिकारकेन्द्रित रिपोर्टिङका लागि आवश्यक ज्ञान र सीप प्रदान गर्ने उद्देश्य राखेको छ । जिम्मेवार डिजिटल पत्रकारितामार्फत मात्र स्वतन्त्र, निष्पक्ष र विश्वसनीय निर्वाचन सुनिश्चित गर्न सकिन्छ, जसले अन्ततः लोकतन्त्रको सुदृढीकरणमा योगदान पुर्‍याउँछ।

४.१. निर्वाचन रिपोर्टिङको संवेदनशीलता र डिजिटल परिवेश

निर्वाचन लोकतान्त्रिक अभ्यासको सबैभन्दा संवेदनशील समय हो, जहाँ सूचनाको सानो त्रुटिले पनि नागरिकको धारणा, मताधिकारको प्रयोग र निर्वाचनको विश्वसनीयतामा गहिरो असर पार्न सक्छ। डिजिटल युगमा यो संवेदनशीलता अझ बढेको छ, किनभने सूचना उत्पादन र प्रसारण अत्यन्त छिटो हुन्छ र सामाजिक सञ्जालमार्फत क्षणभरमै ठुलो जनसमूहसम्म पुग्न सक्छ । यस्तो अवस्थामा पत्रकारले द्रुत समाचार दिने दबाब र तथ्य पुष्टि गर्ने पेसागत जिम्मेवारीबीच सन्तुलन कायम गर्नुपर्छ। निर्वाचन रिपोर्टिङ केवल खबर लेख्ने कार्य मात्र नभई, नागरिकको सूचनाको अधिकार, अभिव्यक्तिको स्वतन्त्रता र निष्पक्ष निर्वाचन सुनिश्चित गर्ने लोकतान्त्रिक जिम्मेवारी पनि हो।

नागरिक तथा राजनीतिक अधिकारसम्बन्धी अन्तर्राष्ट्रिय प्रतिज्ञा पत्र (ICCPR) को धारा १९ ले प्रत्येक व्यक्तिलाई सूचना खोज्ने, प्राप्त गर्ने र प्रवाह गर्ने अधिकार सुनिश्चित गरेको छ । डिजिटल युगमा यो अधिकार इन्टरनेट र डिजिटल प्लेटफर्महरूमार्फत व्यवहारमा लागू हुन्छ । निर्वाचनको समयमा नागरिकहरू

उम्मेदवार, दल, दलको घोषणापत्र र प्रक्रियाबारे जानकारी लिन मुख्यतः डिजिटल मिडियामै निर्भर हुन्छन्। त्यसैले पत्रकारले डिजिटल माध्यम प्रयोग गर्दा सूचनाको अधिकारसँगै गोपनीयता, डाटा सुरक्षा र पहुँचको अधिकारलाई पनि ध्यानमा राख्नुपर्छ । मिथ्या, भ्रामक वा अप्रमाणित सूचना प्रवाह हुनु भनेको केवल पत्रकारिताको कमजोरी मात्र होइन, नागरिकको डिजिटल अधिकारमाथिको उल्लङ्घन पनि हो।

४.२ सुनिश्चितता निर्वाचन रिपोर्टिङमा ध्यान दिनुपर्ने पक्षहरू

क) सूचनाको गुणस्तर सुनिश्चितता

निर्वाचनको समयमा राजनीतिक दल र उम्मेदवारहरू आफ्नो सन्देश मतदातासम्म पुऱ्याउन सक्रिय हुन्छन् भने नागरिकहरू ती सन्देशका आधारमा कसलाई मत दिने निर्णय गर्छन्। यस सम्पूर्ण प्रक्रियामा आमसञ्चार माध्यम प्रमुख सूचना स्रोतको रूपमा रहन्छ। त्यसैले पत्रकारले प्रवाह गर्ने सूचनाको गुणस्तर, सन्तुलन र सन्दर्भ अत्यन्त महत्त्वपूर्ण हुन्छ। राजनीतिक दल वा उम्मेदवारहरूले जानाजानी भ्रामक दाबी, अधूरो तथ्य वा प्रतिस्पर्धीको छवि बिगार्ने सूचना दिन सक्ने सम्भावना रहन्छ। यस्तो अवस्थामा पत्रकारले सूचनाको सत्यता जाँच गर्नु, सन्दर्भ स्पष्ट पार्नु र नागरिकलाई भ्रमित हुन नदिनु आफ्नो पेसागत दायित्वका रूपमा लिनुपर्छ।

ख) स्रोतको प्रयोग, भाषा र पारदर्शिता

निर्वाचनसम्बन्धी समाचार सर्वसाधारण नागरिकले बुझ्ने भाषा र शैलीमा प्रस्तुत हुनुपर्छ । जटिल कानुनी वा प्राविधिक विषयलाई सरल भाषामा व्याख्या गर्नु पत्रकारको सीप हो। डिजिटल प्लेटफर्ममा समाचार प्रकाशित गर्दा स्रोत खुलाउनु अझै महत्त्वपूर्ण हुन्छ, किनभने मिथ्या वा भ्रामक सूचना छिटो फैलिन सक्छ । आधिकारिक स्रोतको उल्लेख, सन्दर्भको स्पष्टता र तथ्यको पुष्टि बिना प्रकाशित समाचारले अन्यौलता र अविश्वास बढाउँछ । यदि कुनै सूचना गोप्य स्रोतबाट आएको हो भने त्यसको कारण बुझेर मात्र प्रयोग गर्नुपर्छ, विशेषगरी उम्मेदवारको

चरित्र वा कानुनी हैसियतसँग सम्बन्धित विषयमा अत्यधिक सावधानी अपनाउनुपर्छ।

ग) समान कभरेज र निष्पक्ष प्रस्तुति

निर्वाचनमा मिडियाले उम्मेदवारलाई कसरी चित्रण गर्छ भन्ने कुराले मतदाताको धारणा निर्माणमा ठुलो भूमिका खेल्छ। त्यसैले पत्रकारले सबै उम्मेदवार र प्रमुख मुद्दालाई समान ध्यान दिनुपर्छ। निष्पक्षताको अर्थ सबैलाई बराबर समय वा स्थान दिनु मात्र होइन, सन्तुलित सन्दर्भ र प्रतिक्रिया समेट्नु पनि हो। यदि एक उम्मेदवारले अर्कामाथि आरोप लगाएको छ भने, आरोपित पक्षको प्रतिक्रिया समावेश गर्नु अनिवार्य हुन्छ। आरोपित पक्षको प्रतिक्रिया नआएमा सोही कुरा स्पष्ट उल्लेख गर्नुपर्छ। पत्रकारले कहिल्यै "कुन उम्मेदवार राम्रो वा नराम्रो" भन्ने निष्कर्ष प्रस्तुत गर्नु हुँदैन; निर्णय गर्ने अधिकार मतदाताको हो।

घ) डिजिटल अभियान, राजनीतिक विज्ञापन र हेरफेरको निगरानी

डिजिटल प्लेटफर्ममा निर्वाचनको समयमा सङ्गठित अनलाइन अभियान, भ्रामक राजनीतिक विज्ञापन र हेरफेर गरिएका सामग्रीहरू तीव्र गतिमा फैलिन्छन्। कतिपय अभियानहरू समन्वित रूपमा चलाइन्छन्, जहाँ एउटै सन्देश धेरै नयाँ वा पहिचान नखुलेका वा बट (Bot) खाताबाट एकै समयमा पोस्ट गरिन्छ। ह्यासट्याग बुस्टिङ, अस्वाभाविक कमेन्टको बाढी र ट्रोल गतिविधि यस्ता अभियानका सङ्केत हुन सक्छन्। पत्रकारले यस्ता गतिविधिलाई पहिचान गरी सन्दर्भसहित रिपोर्ट गर्नुपर्छ, तर त्यस्ता अभियानलाई बढवा दिनमा आफ्नो वा आफ्नो रिपोर्टिङको भूमिका नरहोस् भन्नेमा सावधानी अपनाउनुपर्छ।

ङ) उम्मेदवारविरुद्धको अनलाइन उत्पीडन र घृणास्पद सन्देश

डिजिटल युगमा उम्मेदवारविरुद्धको आक्रमण अब शारीरिक वा मौखिक सीमामा मात्र सीमित छैन; सामाजिक सञ्जालमा गालीगलौज, चरित्र हत्या, लैङ्गिक वा

जातीय घृणास्पद सन्देशमार्फत पनि गरिन्छ । महिला, दलित र अल्पसङ्ख्यक समुदायका उम्मेदवारहरू यस्तो उत्पीडनको उच्च जोखिममा हुन्छन् । पत्रकारले यस्ता घटनालाई सामान्य राजनीतिक आलोचना भनेर उपेक्षा वा सामान्यीकरण गर्नु हुँदैन । सन्दर्भ, उद्देश्य र प्रभाव स्पष्ट पार्दै रिपोर्ट गर्नु, पीडितको गोपनीयता र डिजिटल सुरक्षा ध्यानमा राख्नु, र घृणास्पद सामग्रीलाई पुनः प्रसारण नगर्नु जिम्मेवार डिजिटल पत्रकारिताको दायित्व हो ।

च) निर्वाचनसम्बन्धी मिथ्या तथा भ्रामक सूचना र द्रुत तथ्यजाँच

सामाजिक सञ्जाल सूचना र मिथ्या तथा भ्रामक सूचना दुवैको प्रमुख स्रोत बनेको छ । इन्फ्लुएन्सर, बट (Bot), ट्रोल फार्म (troll farm) र लक्षित अभियान (coordinated campaign) मार्फत मतदाताको धारणा प्रभावित गर्ने प्रयास हुन सक्छ । यस्तो अवस्थामा पत्रकारका लागि द्रुत तथ्यजाँच अनिवार्य सीप हो । सूचनाको स्रोत को हो, किन अहिले भाइरल भयो, फोटो वा भिडियो पुरानो त होइन, सन्दर्भ मिल्छ कि मिल्दैन लगायतका प्रश्नहरूको उत्तर खोजेर मात्र समाचार प्रकाशित गर्नुपर्छ । अन्य विश्वसनीय मिडियाले पनि सोही सूचना वा समाचार प्रसारण गरेको छ कि छैन भन्ने जाँचले समाचारको विश्वसनीयता बढाउँछ ।

छ) मतदाता र संवेदनशील डाटाको सुरक्षा

निर्वाचन रिपोर्टिङमा मतदाता नामावली, बुथस्तरको नतिजा, मतदान प्रवृत्ति जस्ता डाटा प्रयोग गरिन्छ । यस्ता डाटा प्रयोग गर्दा पत्रकारले गोपनीयता र डाटा सुरक्षालाई प्राथमिकता दिनुपर्छ । व्यक्तिगत रूपमा पहिचान गर्न सकिने विवरण (नाम, ठेगाना, नागरिकता नम्बर) प्रत्यक्ष प्रकाशित गर्नु हुँदैन । आवश्यक परेमा तथ्याङ्कीय (aggregated) रूपमा मात्र प्रस्तुत गर्नुपर्छ । डिजिटल फाइलहरू सुरक्षित रूपमा भण्डारण गर्नु, आवश्यक नभएपछि नष्ट गर्नु र स्रोत तथा सीमाबारे स्पष्ट जानकारी दिनु जिम्मेवार पत्रकारिताको आधार हो ।

ज) स्रोतको गोपनीयता र सूचित सहमति

निर्वाचनको समयमा धेरै स्रोतहरू उच्च जोखिममा हुन सक्छन्। यदि स्रोतले आफ्नो नाम गोप्य राख्न चाहन्छ भने पत्रकारले त्यसको डिजिटल र भौतिक सुरक्षा सुनिश्चित गर्नुपर्छ। स्रोतको पहिचान खुल्ने विवरणहरू सामान्यीकरण गर्नु, इन्क्रिप्टेड भण्डारण प्रयोग गर्नु र अफलाइन सुरक्षा अपनाउनु आवश्यक हुन्छ। साथै, स्रोतसँग सूचित सहमति लिनु, उनीहरूको जानकारी कसरी प्रयोग हुनेछ, के कस्तो जोखिम हुन सक्छ आदि विषयमा सबै कुरा स्पष्ट रूपमा छलफल गर्नु नैतिक र पेसागत दायित्व हो।

४.३ प्रेस स्वतन्त्रता, तटस्थता र डिजिटल दबाबको व्यवस्थापन

नेपालको संविधानले प्रेस स्वतन्त्रता र अभिव्यक्ति स्वतन्त्रतालाई मौलिक अधिकारका रूपमा सुनिश्चित गरेको छ। तर व्यवहारमा, विशेषगरी निर्वाचनजस्ता संवेदनशील समयमा, पत्रकारहरूले विभिन्न किसिमका प्रत्यक्ष र अप्रत्यक्ष दबाबको सामना गर्नुपर्छ। डिजिटल युगमा यी दबाबको स्वरूप र तीव्रता दुवै परिवर्तन भएका छन्। विगतमा पत्रकार वा मिडियालाई फोन गरेर वा प्रत्यक्ष रूपमा धम्की दिने, विज्ञापन रोक्ने चेतावनी दिने वा कार्यालयमै पुगेर हुलहुज्जत गर्ने प्रवृत्ति देखिन्थ्यो भने अहिले अनलाइन ट्रोलिङ, सङ्गठित सामाजिक सञ्जाल आक्रमण, अनफलो अभियान, साइवर अपराधमा उजुरीको धम्की र कहिलेकाहीँ अकाउन्ट ह्याकिङ वा डक्सिङ (doxxing) जस्ता डिजिटल आक्रमण हुन थालेका छन्।

निर्वाचनको समयमा पत्रकारले तयार पारेका समाचार, विश्लेषण वा तथ्यजाँच शक्तिशाली राजनीतिक दल, उम्मेदवार वा स्वार्थ समूहलाई चित्त नबुझ्न सक्छ। त्यसको प्रतिक्रियामा पत्रकारलाई लक्षित गरी सामाजिक सञ्जालमा गाली बेइज्जति, चरित्र हत्या, लैङ्गिक वा जातीय अपमान, झूटा आरोप र धम्कीहरू फैलाइने प्रवृत्ति देखिन्छ। यस्ता आक्रमणहरू प्रायः कुनै समूहको संयोजनमा भएका हुन्छन् र यसअन्तर्गत पहिचान नखुलेका वा बट वा नयाँ अकाउन्टहरूको प्रयोग गरी एकै प्रकृतिका सन्देश प्रवाह गरिन्छ। यस्तो संयोजित आक्रमणहरूले

पत्रकारमाथि मानसिक दबाब सिर्जना गर्नुका साथै स्वनियन्त्रण (self-censorship) तर्फ धकेल्न सक्छ।

पछिल्लो चरणमा पत्रकारहरूका लागि डिजिटल वातावरणमा तटस्थता कायम राख्ने काम थप जटिल भएको छ। सामाजिक सञ्जालमा देखिने "ट्रेन्ड", लाइक, शेयर वा कमेन्टको सङ्ख्या पत्रकारका लागि लोकप्रियताको मापदण्ड जस्तो देखिन सक्छ। तर डिजिटल भीडको यस्तो दबाबले समाचारको प्राथमिकता र कोण (angle) नै बदलिन सक्ने जोखिम रहन्छ। व्यक्तिगत राजनीतिक धारणा, सामाजिक सञ्जालमा व्यक्त गरिएको मत वा कुनै पक्षको व्यापक समर्थन देखिएको कारणले समाचारको तथ्य, सन्तुलन र सन्दर्भ प्रभावित हुनु हुँदैन। पत्रकारले आफ्ना व्यक्तिगत डिजिटल गतिविधि र पेसागत रिपोर्टिङबीच स्पष्ट सीमा (professional boundary) कायम गर्न आवश्यक हुन्छ।

डिजिटल दबाब व्यवस्थापनका लागि डिजिटल सुरक्षा र पेसागत अभ्यास एकअर्कासँग जोडिएका छन्। पत्रकारले आफ्ना अनलाइन अकाउन्टहरू सुरक्षित राख्नु, दुई तह प्रमाणीकरण (two-factor authentication) प्रयोग गर्नु, शङ्कास्पद लिङ्क वा फाइल नखोल्नु, र संवेदनशील संवादका लागि सुरक्षित माध्यम प्रयोग गर्नु आवश्यक हुन्छ। यसले ह्याकिङ, डाटा चोरी वा मिथ्या वा भ्रामक सूचना फैलाउने जोखिम घटाउँछ। साथै, अनलाइन उत्पीडनको अवस्थामा प्रमाण सुरक्षित राख्ने (स्क्रिनसट, URL, मिति, समय) र आवश्यक परे संस्थागत वा कानुनी सहयोग लिनु पनि महत्त्वपूर्ण हुन्छ।

अन्ततः, पत्रकारको सबैभन्दा बलियो सुरक्षा भनेकै तथ्यमा आधारित, सन्तुलित र प्रमाणसहितको रिपोर्टिङ हो। जब समाचार स्पष्ट स्रोत, प्रमाण र सन्दर्भमा आधारित हुन्छ, त्यस्ता समाचारमाथि हुने डिजिटल आक्रमणको नैतिक र कानुनी पक्ष कमजोर हुन्छ। मिडिया हाउसको संस्थागत समर्थन, सहकर्मीबीचको एकता, र पेसागत आचारसंहिताप्रतिको प्रतिबद्धताले मात्र पत्रकारले डिजिटल दबाबका बाबजुद आफ्नो स्वतन्त्रता र तटस्थता जोगाउँदै लोकतान्त्रिक भूमिकालाई निरन्तरता दिन सक्छन्।

४.४ निष्कर्ष

डिजिटल युगमा निर्वाचन रिपोर्टिङ केवल समाचार उत्पादन वा सूचना प्रवाहको प्रक्रिया मात्र होइन; यो डिजिटल अधिकारको सम्मान र संरक्षण, लोकतान्त्रिक मूल्यहरूको सुदृढीकरण, तथा पत्रकारको पेसागत इमानदारी र उत्तरदायित्वको प्रत्यक्ष परीक्षा हो। तीव्र सूचना प्रवाह, सामाजिक सञ्जालको प्रभाव, र डिजिटल जोखिमहरूको बीचमा पत्रकारले सत्यता, निष्पक्षता र सुरक्षा कायम राख्नु अझ चुनौतीपूर्ण बनेको छ। यस्तो परिवेशमा तथ्यमा आधारित, सन्तुलित, सुरक्षित र अधिकार केन्द्रित रिपोर्टिङले मात्र नागरिकलाई सही सूचना प्रदान गर्न सक्छ, सार्वजनिक विश्वास कायम गर्न सक्छ, र निर्वाचन प्रक्रियालाई पारदर्शी तथा विश्वसनीय बनाउन सार्थक योगदान दिन सक्छ। पत्रकारिताको यही जिम्मेवार अभ्यास नै लोकतान्त्रिक समाजको आधार र डिजिटल युगको सशक्त प्रेसको पहिचान हो।

परिच्छेद ४

सहयोगी सामाग्री, उपकरण र चेकलिस्ट

५.१ प्रमाणीकरण र तथ्यजाँच प्लेटफर्महरू

प्रमाणीकरण क्रियाकलाप	उपकरण / प्लेटफर्म	लिङ्क	प्रयोग / उद्देश्य/टिप्पणी
Reverse Image Search	TinEye	https://www.tineye.com/	तस्बिरको पहिलो प्रयोग, पुरानो सन्दर्भ पत्ता लगाउन/Image manipulation पहिचानमा उपयोगी
	Google Lens	https://lens.google/	तस्बिरको स्रोत, मिल्दोजुल्दो सामग्री खोज्न/ सबैभन्दा सजिलो र व्यापक
	Google Reverse Image Search	https://images.google.com/	तस्बिरको स्रोत, मिल्दोजुल्दो सामग्री खोज्न
	Yandex Image Search	https://yandex.com/images/	वैकल्पिक र विस्तृत खोज नतिजा प्राप्त गर्न
	Bing Visual Search	www.microsoft.com/en-us/bing/visual-search	तस्बिर र वस्तु पहिचान/ Google को विकल्प

भिडियो प्रमाणीकरण	InVID -WeVerify	https://cedmohub.eu/invid-weverify-verification-plugin/	भाइरल भिडिओलाई Key-frames मा विभाजन गरी प्रमाणीकरण/ Deepfake पहिचानमा उपयोगी
	YouTube Data Viewer | YTLarge	https://v2.ytlarge.com/data-viewer	YouTube भिडियोको अपलोड मिति, थम्बनेल जाँच/ पुराना भिडिओ पुनः प्रयोग भएको पत्ता लगाउन उपयोगी
	Frame by Frame (VLC Player)	https://chromewebstore.google.com/detail/frame-by-frame/cclnaabdfgne-hogonpeddbgej-clcjneh	भिडियोको फ्रेम-स्तर विश्लेषण/ Edit गरिएको भिडियो पत्ता लगाउन उपयोगी
समाचार प्रमाणीकरण (नेपाल केन्द्रित)	Nepal Check	https://nepalcheck.org/	नेपालसम्बन्धी दाबी र अफवाहको तथ्यजाँच/ स्थानीय सन्दर्भका लागि उपयोगी
	Nepal Fact Check	https://nepalfact-check.org/	राजनीतिक र सामाजिक समाचार प्रमाणीकरण
	TechPana Fact Check	https://techpana.com/factcheck/	प्रविधि र डिजिटल अफवाह जाँच
	The Ruju	https://theruju.com/	दाबी, भाषण र समाचारको विस्तृत जाँच
	News-Checker Nepal	https://nepal.newschecker.co/en	चुनाव, राजनीति र सामाजिक मिडिया अफवाह जाँच

भाषण / दाबी प्रमाणीकरण	Google Fact Check Explorer	https://toolbox.google.com/factcheck/explorer/search/list:recent;hl=en	दाबी पहिल्यै fact-check भएको छ कि छैन जाँच/ अन्तर्राष्ट्रिय र क्षेत्रीय स्रोत पत्ता लगाउन उपयोगी
	ClaimReview Markup Search	https://developers.google.com/search/docs/appearance/structured-data/factcheck	संरचित fact-check डाटा खोज/ अनुसन्धानका लागि उपयोगी
सोशल मिडिया विश्लेषण	OSoMeNet	https://osome.iu.edu/tools/osomenet/	सामाजिक सञ्जालहरुमा सूचना कसरी फैलिराखेको छ भन्ने भिजुअलाइज गर्न
	TweetDeck / X Advanced Search	http://twitter.com/search-advanced	X (Twitter) पोस्ट खोज र विश्लेषण/ पुराना पोस्ट पत्ता लगाउनका उपयोगी
डिजिटल प्रमाण संरक्षण	Archive.today	https://archive.ph/	डिलिट भएको पोस्ट/पेज सुरक्षित राख्न/ कानुनी प्रमाण राख्नका लागि उपयोगी
	Wayback Machine	https://web.archive.org/	वेबसाइटको पुरानो संस्करण हेर्न/ नीति/घोषणा परिवर्तन ट्र्याक गर्नेका लागि उपयोगी
	Perma.cc	http://Perma.cc	स्थायी link सिर्जना गरी प्रमाण सुरक्षित/ कानुनी अनुसन्धानमा उपयोगी

Deepfake / AI सामग्री पहिचान	AI or Not	https://www.aiornot.com/	AI-generated image जाँच/ प्रारम्भिक सङ्केतका लागि उपयोगी
	Hive Moderation	https://hivemoderation.com/	AI-generated text/image/ video पहिचान/ Advanced detection
	Reality Defender	https://www.realitydefender.com/	Deepfake video/audio जाँच/ उच्च जोखिम केसका लागि उपयोगी
	WaistAI	https://wasitai.com/	भिडियोको स्क्रीनसटमा एआई प्रयोग भएको छ कि छैन जाँच/ प्राथमिक स्तरको जाँच
	Deepfake classifier	https://github.com/topics/deepfakes-classification	AI-generated content पहिचान
	ImageWhisperer	https://imagewhisperer.org/	भिडियो वा फोटो वास्तविक भएको पुष्टि
मेटाडाटा विश्लेषण	Exif.tools	https://exif.tools/	तस्बिर/फाइलको metadata जाँच / Location, device जाँच
	Metadata-2Go	(https://www.metadata2go.com/)	
	FotoForensics	https://fotoforensics.com/	Image manipulation (ELA) जाँच/ फोटो इडिट पहिचान

भौगोलिक प्रमाणीकरण (Geolocation)	Google Maps / Street View	https://www.google.com/streetview/	स्थान प्रमाणीकरण/ दृश्य मिलान
	OpenStreetMap	https://www.openstreetmap.org/#map=7/28.415/84.128	वैकल्पिक नक्सा प्रमाणीकरण
	SunCalc	https://www.suncalc.org/	छायाको आधारमा समय/स्थान जाँच/ Advanced verification
डोमेन / वेबसाइट जाँच	WHOIS Lookup	https://www.whois.com/whois/	वेबसाइट कसले र कहिले दर्ता गर्‌यो जाँच/ Fake news साइट पहिचान
	BuiltWith	https://builtwith.com/	वेबसाइटको टेक्निकल प्रोफाइल/ Coordinated network जाँच

सन्दर्भ सामग्री

- Media Helping Media. *Respecting privacy as a journalist. https://mediahelpingmedia.org/ethics/respecting-privacy-as-a-journalist/*
- Centre for Media Rights. *पत्रकारको अधिकार र जिम्मेवारी http://www.cmr.org.np/book.pdf*
- Africa Check. (2024). *Youth media literacy fact-checking manual*. Internews.*https://internews.org/wp-content/uploads/2024/02/Youth-Media-Litreracy-Program-Fact-Checking-Manual-final.pdf*
- Pogorelec, A. (2025, March 13). *How to secure your personal metadata from online trackers.* Help Net Security. *https://www.helpnetsecurity.com/2025/03/13/how-to-protect-personal-metadata/*
- WhatIsMyIPAddress.com. (n.d.). *Do virtual machines protect your privacy better?*.
- *https://whatismyipaddress.com/do-virtual-machines-protect-your-privacy-better*
- FTK-Centre for Information Technology, Jamia Millia Islamia. (n.d.). *Cyber security: Some suggested dos & don'ts. https://www.jmi.ac.in/upload/menuupload/cit_cybersecurity_dosanddonts.pdf*

अनुसुची -१

प्रेस काउन्सिल नेपालले जारी गरेको पत्रकार आचारसंहिता, २०७३ (पहिलो संशोधन २०७६)[7] मा अनलाइन सञ्चार माध्यममा लागु हुने मुख्य प्रावधानहरु:

२(१) "अनलाइन सञ्चारमाध्यम भन्नाले प्रचलित कानुनबमोजिम स्थापना भई पत्रकारिता र सम्पादकीय सिद्धान्त अगिंकार गर्दै इन्टरनेटको माध्यमबाट सकेन, चिन्ह, अक्षर, आवाज, ग्राफिक्स, मिडिया, एनिमेशन तथा विभिन्न बहुमाध्यम (मल्टिमिडिया को प्रयोगमार्फत समाचारमूलक वा विषयगत विचार, सूचना तथा समाचार, तस्विर, श्रव्यदृश्यको रुपमा उत्पादन, प्रकाशन, प्रसारण वा वितरण गर्ने विधि, प्रक्रिया माध्यम सम्झनु पर्छ ।

२(८) "प्रसारण" भन्नाले, इन्क्रीप्ट (encrypt) गरिएको वा नगरिएको, सर्वसाधारण वा निश्चित क्षेत्र वा वर्गका जनताले जानकारी पाउन सक्ने गरी पठाइने श्रव्य वा दृष्य, श्रव्यदृष्य, कार्यक्रम, डाटा वा सूचनालाई रेडियो फ्रिक्वेन्सी, इण्टरनेट प्रोटोकल वा अन्य विद्युतीय वा विद्युत प्रकाशीय (optical) माध्यमबाट गरिने प्रसारण सम्झनु पर्छ ।

२(११) 'सञ्चारमाध्यम' भन्नाले नेपालमा सञ्चालित छापामाध्यम, रेडियो, टेलिभिजन, अनलाइन सञ्चारमाध्यम र समाचार एजेन्सीलाई सम्झनुपर्छ ।

४(१) पत्रकार तथा सञ्चारमाध्यमले नागरिकको आधारभूत अधिकार, विचार तथा अभिव्यक्ति स्वतन्त्रताको संरक्षण र संवर्द्धनका निम्ति सदैव सत्य तथ्य सूचना प्रवाह गर्नुपर्दछ ।

४(६)(१) पत्रकार तथा सञ्चारमाध्यमले सत्य तथ्य र सन्तुलित समाचार सामग्री सम्प्रेषण गर्नुपर्दछ । यसरी सम्प्रेषण गर्दा सम्बन्धित पक्षको भनाइलाई उचित स्थान दिनु पर्दछ ।

---

7 https://www.presscouncilnepal.gov.np/np/wp-content/uploads/2019/09/code-of-conduct-2076.pdf

४(६)(२) पत्रकार तथा सञ्चारमाध्यमले सामाजिक सञ्जालमार्फत् प्रवाह गर्ने समाचार, विचार र सूचना वा जानकारीहरू सत्य तथ्यपूर्ण, सन्तुलित र मर्यादित हुनु पर्दछ ।

४(६)(३) सामाजिक सञ्जालका अन्य प्रयोगकर्ताहरूले प्रकाशन गरेको जानकारी वा विचार/कमेन्टहरूलाई शेयर वा रिट्विट गरी पुन प्रकाशन गर्दा पत्रकार तथा सञ्चारमाध्यमले आफूले प्रकाशन गरे सरह तथ्यजाँच गरी निष्पक्षतालाई समेत ख्याल गरी सम्प्रेषण गर्नुपर्दछ ।

४(७) समाचार, विचार र विज्ञापन छुट्टिने गरी सम्प्रेषण: १) पत्रकार तथा सञ्चारमाध्यमले पाठक, श्रोता वा दर्शकमा भ्रम वा संशय उत्पन्न नहुने गरी समाचार, लेख, विचार र प्रायोजित सामग्री वा विज्ञापनवीच स्पष्ट अन्तर हुनेगरी सम्प्रेषण गर्नु, गराउनुपर्दछ ।

४ (९) गोपनीयताको हकको सम्मान पत्रकार तथा सञ्चारमाध्यमले व्यक्तिको गोपनीयताको हकको सम्मान गर्नुपर्दछ । तर सार्वजनिक हितमा त्यस्तो सूचना वा सामग्री सम्प्रेषण भएमा गोपनीयताको हकको सम्मान प्रतिकूल भएको मानिनेछैन ।

४ (१४) (१) पत्रकार तथा सञ्चारमाध्यमले समाचार तथा विज्ञापन सम्प्रेषण गर्दा सार्वजनिक सरोकार र संवेदनशीलतालाई सदैव ख्याल गर्नुपर्दछ। त्यस्ता सामग्रीको सत्यतामाथि प्रश्न उठ्नासाथ अनुसन्धान गर्नु, त्रुटि एवं गल्ती भएको जानकारी हुनासाथ यथाशीघ्र सच्याउनु तथा प्रकाशित वा प्रसारित सामग्री असत्य हो भन्ने सप्रमाण खण्डन वा प्रतिक्रिया आएमा प्रष्ट भाषामा उचित स्थान दिई प्रकाशन वा प्रसारण गर्नुपर्दछ ।

४ (१४) (२) सामान्यतः कुनै एउटा सञ्चारमाध्यमबाट प्रकाशित वा प्रसारित समाचारको खण्डन पीडित पक्षले सोही सञ्चारमाध्यममार्फत गर्नुपर्दछ । तर, सार्वजनिक स्वास्थ्य र सुरक्षा जस्ता संवेदनशील विषयमा तत्काल गम्भीर असर पार्ने अवस्थामा भने अन्य सञ्चारमाध्यम मार्फत् खण्डन, टिप्पणी वा स्पष्ट गर्न सकिनेछ ।

अनुसुची -२

निर्वाचन आयोगद्वारा प्रकाशित निर्वाचन आचारसंहिता, २०८२[8]

निर्वाचन आयोगद्वारा प्रकाशित निर्वाचन आचारसंहिता, २०८२ मा दफा २५ मा सञ्चार प्रतिष्ठान, सम्बद्ध कर्मचारी तथा पत्रकारले पालना गर्नुपर्ने आचरणहरु के के रहने भनेर उल्लेख गरेको छ।

२५. सञ्चार प्रतिष्ठान, सम्बद्ध कर्मचारी तथा पत्रकारले पालना गर्नुपर्ने आचरण:

(१) सञ्चार प्रतिष्ठान, सोमा सम्बद्ध कर्मचारी तथा पत्रकारले देहायका आचरण पालन गर्नु पर्नेछः-

(क) कुनै राजनीतिक दल वा उम्मेदवार वा निजको प्रतिनिधिबाट दान, उपहार वा आर्थिक सहयोग लिन नहुने,

(ख) कसैको पक्ष वा विपक्षमा समाचार प्रकाशन वा प्रसारण गर्न हुँदैन ।

(ग) जातजाति, भाषा, धर्म, सम्प्रदाय, लिङ्ग र क्षेत्र बीचको सम्बन्ध र सद्भावमा खलल पार्ने, राजनीतिक आस्था वा विचार, राष्ट्रियता तथा सामाजिक अवस्था जस्ता कुनै पनि आधारमा भेदभाव हुने गरी समाचार प्रकाशन वा प्रसारण गर्न नहुने,

(घ) राजनीतिक दल वा उम्मेदवारको निर्वाचन प्रचार प्रसारको लागि निःशुल्क विज्ञापन प्रकाशन, प्रसारण वा सम्प्रेषण गर्न नहुने,

(ङ) दफा १५ बमोजिम राजनीतिक दल वा उम्मेदवारको निर्वाचन सम्बन्धी विज्ञापन प्रकाशन, प्रसारण वा सम्प्रेषण गर्दा सो विज्ञापनमा सःशुल्क भएको जनाउ दिनु पर्ने,

तर मतदान हुने दिनको अघिल्लो अठचालिस घण्टादेखि मतदानको दिन मतदान केन्द्र बन्द नहुन्जेलसम्म त्यस्तो विज्ञापन प्रकाशन, प्रसारण वा सम्प्रेषण गर्न पाइने छैन।

8 https://election.gov.np/

(च) कसैको पक्ष वा विपक्षमा एस.एम.एस., सामाजिक सञ्जाल, अनलाइन छापा जस्ता विद्युतीय माध्यममा आर्टिफिसियल इन्टिलिजेन्स (ए.आइ.) को प्रयोग गरी वा नगरी कुनै सामग्री प्रकाशन, प्रसारण वा सम्प्रेषण गर्न तथा त्यस्ता सामग्री सामाजिक सञ्जालमा पोस्ट, रिपोस्ट, शेयर, कमेन्ट वा प्रतिकमेन्ट, लाइभ स्ट्रिमिङ, ट्याग वा मेन्सन लगायतका कार्य गर्न वा गराउन नहुने,

(छ) सूचनाको स्रोतको गोपनीयता भङ्ग गर्न नहुने,

(ज) राजनीतिक दल वा उम्मेदवार तथा उम्मेदवारको एकाघरका परिवारका सदस्यको मान, प्रतिष्ठा, इज्जतमा आँच पुऱ्याउने तथा मिथ्या र भ्रामक समाचार प्रकाशन तथा प्रसारण गर्न नहुने,

(झ) मतदान हुने दिनको अघिल्लो अठचालिस घण्टादेखि मतदानको दिन मतदान केन्द्र बन्द नहुन्जेलसम्म राजनीतिक दल वा उम्मेदवारको पक्ष वा विपक्षमा विज्ञापनका अतिरिक्त टक सो, टिप्पणी, विश्लेषण, प्रश्नोत्तर जस्ता कार्यक्रम गर्न नहुने,

(ञ) निर्वाचनको बारेमा नकारात्मक सन्देश प्रवाह गर्ने लेख, तस्वीर वा समाचार प्रकाशन वा प्रशारण गर्न नहुने,

(ट) नेपालको निर्वाचन, राजनीतिक दल र उम्मेदवारलाई नकारात्मक असर पुग्ने गरी विदेशी सञ्चार माध्यमबाट प्रकाशित वा प्रसारित सामग्री पुनः प्रकाशन वा प्रशारण गर्न नहुने, र

(ठ) कसैले निर्वाचनलाई प्रभाव पार्ने उद्देश्यले होच्याउने, दुष्प्रचार गर्ने, अपमान गर्ने, मिथ्या सूचना, द्वेषपूर्ण भाषण (हेट स्पिच), जस्ता भ्रामक टिका टिप्पणी इन्टरनेट वा टेलिभिजनमा सम्प्रेषण गर्न नहुने र त्यस्तो टिकाटिप्पणी सम्प्रेषण भएमा इन्टरनेट सेवा प्रदायक वा केबल टेलिभिजन वितरकले त्यस्ता सूचना वा अभिव्यक्तिलाई हटाउनु पर्ने।

(२) यस आचारसंहिताको अधिनमा रही कुनै पनि सञ्चार संस्था वा सञ्चार गृहले आफ्नो संस्थामा कार्यरत पत्रकार, स्ट्रिन्जर, क्रु मेम्बर र कर्मचारीलाई निर्वाचनसम्बन्धी स्वःआचारसंहिता बनाइ लागू गर्न सक्नेछन् ।

Digital Rights Nepal

डिजिटल राइट्स नेपाल

निल सरस्वती मार्ग, गैरीधारा, काठमाडौं
फोनः ९७७-९७६७२४५१००
इमेलः info@digitalrightsnepal.org
www.digitalrightsnepal.org

नेपाल पत्रकार महासंघ

मिडिया भिलेज, सञ्चारग्राम, काठमाडौं
फोनः ९७७-१-५९१४७८५
इमेलः fnjnepalcentral@gmail.com
वेबसाइटः www.fnjepal.org