भारत सरकार में साइबर सुरक्षा और डेटा गोपनीयता द्वारा डिजिटल सम्पतियों की सुरक्षा

भूमंडलीकरण के इस दौर में जहाँ दुनिया के देशों में उत्तरोतर संपर्क ने उनके अंतर्संबंधों को संबल दिया है वहीं इन्टरनेट के माध्यम से डेटा अंतरण ने महत्वपूर्ण विषयों की सुरक्षा को संवेदनशील बनाया है। इससे छुटकारा पाने में साइबर सुरक्षा एक महत्वपूर्ण विषय के रूप में उभर कर सामने आया है जिसके औपचारिक और अनौपचारिक आयाम विचारणीय हैं। साइबर सुरक्षा में सिस्टम, नेटवर्क और प्रोग्राम को डिजिटल हमलों से बचाने के लिए प्रौद्योगिकियों और प्रक्रियाओं का उपयोग करता है जिससे डेटा की गोपनीयता और सुरक्षा बरक़रार रहे। साइबर सुरक्षा मुख्य रूप से कंप्यूटर, सर्वर, मोबाइल डिवाइस, इलेक्ट्रॉनिक सिस्टम, नेटवर्क और डेटा को शत्रुतापूर्ण हमलों से बचाने की एक प्राविधि भी है। समकालीन समाज में लोगों, उपकरणों और कार्यक्रमों की बढ़ती संख्या के साथ- साथ डेटा की बढ़ती बाढ़ ने साइबर सुरक्षा के महत्त्व को स्वीकार किया है । सम्प्रति, साइबर सुरक्षा का महत्व इसलिए भी बढ़ गया है क्योंकि लोक कल्याणकारी योजनाओं में लोगों के व्यक्तिगत और निजी आकड़ों को डिजिटिल माध्यमों में संग्रहित किया जाने लगा है ताकि सरकारी नीतियों को अधिक जनोपयोगी बनाया जा सके। साथ ही साथ, डिजिटलीकरण के माध्यम से सरकारी रिकार्ड्स भी डिजिटलकृत किए जा रहें हैं। डिजिटलकृत आकड़ों का इतना महत्त्व बढ़ गया है कि इन्हें 21 शताब्दी की मुद्रा भी कहा जाने लगा है। वस्तुतः हमारे दैनिक जीवन के उपयोग में लाए जाने वाले मोबाइल फोन एप्स ने उपभोग और उत्पादन के क्षेत्र में उपभोक्ताओं के मनोवृतियों का विश्लेषण भी सुलभ कर लिया है। गूगल, फेसबुक तथा अमेज़न जैसी ऑनलाइन सेवा प्रदान करने वाली कंपनियों ने डेटा अर्थव्यवस्था के माध्यम से अपने महत्त्व को बढ़ा लिया है।

आज के समय में डेटा का चलन मुद्रा के समतुल्य माना जाने लगा है अतः डेटा की चोरी या उसके साथ छेड़-छाड़ डेटा अपराधी करने लगें हैं। इन अपराधियों से डेटा को बचाना ही साइबर सुरक्षा है। साइबर सुरक्षा (Cyber Security) वह तकनीकी सुरक्षा है जिसे इंटरनेट, कंप्यूटर सिस्टम, नेटवर्क और डेटा को सुरक्षित रखने के लिए डिज़ाइन की जाती है। इसका मुख्य उद्देश्य अनाधिकृत एक्सेस, डेटा चोरी, नुकसान, डेटा असुरक्षा के खिलाफ सुरक्षा उपायों का अनुसरण करना है। साइबर सुरक्षा के क्षेत्र में कई तरह के हमले होते रहते हैं जैसे मैलवेयर, फिशिंग, डिनायल ऑफ सर्विस (DoS), डेटा ब्रीच, और डेटा थेफ़्ट आदि। इन हमलों

से बचाव के लिए विभिन्न सुरक्षा उपकरणों को प्रयोग में लाया जाता है, जैसे कि फ़ायरवॉल, एंटीवायरस सॉफ़्टवेयर, एंटी-स्पैम फ़िल्टर, तथा नवीन सृजित प्रविधियां।

'सामान्य डेटा संरक्षण अधिनियम 2016' (General Data Protection Regulation, GDPR) यूरोपीय संघ द्वारा बनाई गई एक महत्वपूर्ण नीति है जो 25 मई 2018 से पूरे यूरोपीय संघ में लागू की गयी है। यह नीति उपयोगकर्ताओं के व्यक्तिगत डेटा की सुरक्षा और उनकी गोपनीयता को सुनिश्चित करने के लिए संकल्पित है। उपयोगकर्ताओं को उनके व्यक्तिगत डेटा पर नियंत्रण का अधिकार, डेटा की सुरक्षा में लापरवाही करने पर कठोर दंड का प्रावधान, डेटा ब्रीच की स्थिति में ग्राहकों और नियामक संगठनों को सूचना देने का अधिकार आदि मुख्य हैं। भारत सरकार ने भी साइबर सुरक्षा नीति 2013 को लागू किया है जिसमे साइबर सुरक्षा के क्षेत्र में राष्ट्रीय नीतियों और दिशानिर्देशों को संज्ञान में लिया गया है। इसके अंतर्गत साइबर हमलों की पहचान और उनकी रोकथाम के लिए उपायों को भी अभिदार्शित किया गया है। राष्ट्रीय साइबर सुरक्षा नीति (National Cyber Security Policy) का उद्देश्य एक सुरक्षित कंप्यूटर वातावरण के निर्माण की सुविधा प्रदान करना और इलेक्ट्रॉनिक लेन- देन में पर्याप्त विश्वास और विश्वास को सक्षम करने के साथ-साथ साइबर स्पेस सुरक्षा के लिए हितधारकों की गतिविधियों का मार्गदर्शन करना है।

साइबर सुरक्षा और डेटा गोपनीयता के सन्दर्भ में मुख्य घटक (1) साइबर धोखाधड़ी की रोकथाम (2) डिजिटल सार्वजनिक बुनियादी ढांचा (3) डेटा स्थानीयकरण (4) डिजिटल सुरक्षा और ब्लाकचेन सुरक्षा (5) गोपनीयता (6) घटना प्रतिक्रिया योजना सम्बन्धी नियम व प्रावधान (7) अंतर्राष्ट्रीय सहयोग (8) जागरूकता और शिक्षा, तथा (9) निरंतर निगरानी और अनुकूलन हैं।

भारत में सरकारी तथा निजी कंपनियां बैंकिंग और बाज़ार सहित लगभग हर क्षेत्र में जिसमें डिजिटल क्षेत्र भी शामिल है, आगे बढ़ रहीं हैं। वर्त्तमान में आर्टिफिशियल इंटेलिजेंस (AI) ने भी तेजी से पांव फैलाना शुरू किया है। इसके परिणामस्वरुप डेटा ऑनलाइन गतिविधियाँ भी रिकॉर्ड होने लगीं हैं। इस सन्दर्भ में कुछ प्रमुख विन्दुओं पर ध्यान दिया जाना आपेक्षित है, जैसे:

1. क्या साइबर सुरक्षा उपभोक्ताओं के हितों की पूर्ण रक्षा कर पा रहें हैं?
2. क्या डेटा का उपयोग विवेकपूर्ण ढंग से केवल उसी उद्देश्य से किया जा रहा है जिसके लिए एकत्र किया गया था?

3. क्या उपभोक्ता आर्टिफिशियल इंटेलिजेंस और डेटा एनालिटिक्स के अवसर और चुनौतियों से पूर्ण रूप से अवगत है ?
4. व्यक्तिगत निजता और राष्ट्रीय सुरक्षा पर अंतरराष्ट्रीय खतरा क्या है ?
5. साइबर युद्ध में राज्य और गैर राज्य अभिकरणों की क्या भूमिका है ?

विदित हो कि भारत ने पिछले वर्षों की तुलना में 2022 में रिपोर्ट किए गए साइबर अपराधों में उल्लेखनीय उछाल देखा है । इस वर्ष साइबर अपराध की 65 हजार से अधिक घटनाएं दर्ज की गई थीं। मापी गई समयावधि के दौरान कर्नाटक और तेलंगाना की हिस्सेदारी सबसे अधिक रही। भारत के राज्य कर्नाटक में साइबर अपराध के क्षेत्र में आईटी अधिनियम के तहत धोखाधड़ी और पीड़ितों का यौन शोषण पाया गया। वर्ष 2022 में, तेलंगाना राज्य में देश के बाकी हिस्सों की तुलना में साइबर अपराधों की सबसे अधिक संख्या दर्ज की गई थी, जिसमें औपचारिक रूप से 15 हजार से अधिक मामले दर्ज किए गए थे।

बढ़ती डिजिटल अर्थव्यवस्था ने हमारे दैनिक जीवन में उच्च जटिलता या डिजिटल पहलुओं के दायरे को बढ़ा कर साइबर अपराधियों के लिए नए अवसर पैदा किए हैं। उदाहरण के लिए, 2021 में पूरे भारत में साइबर अपराध के लिए गिरफ्तार किए गए और आरोपित किए गए लोगों की संख्या ने अपराधिक आरोपों की एक विस्तृत स्पेक्ट्रम दिखाई, जिसमें ब्लैकमेलिंग, जालसाजी, यौन शोषण तथा जालसाजी प्रमुख थे।

ऐसी स्थिति में डिजिटल सुरक्षा एवं गोपनीयता यक्ष प्रश्न के रूप में सामने खड़े हैं। लोक प्रशासन के इस विशेषांक में उपर्युक्त के आलोक में शोध पत्र आमंत्रित किए जातें हैं।