अधिसूचना

नई दिल्ली, 27 अक्तूबर, 2009

सा.का.नि. 782(अ).— केंद्रीय सरकार सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 69क की उपधारा (3) के साथ पठित, धारा 87 की उपधारा (2) के खंड (यक) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए निम्नलिखित नियम बनाती है, अर्थात, :

1. **संक्षिप्त नाम और प्रारंभ** – (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (ट्रैफिक आंकड़ों या सूचना को मानीटर और एकत्रित करने के लिए प्रक्रिया और रक्षोपाय) नियम, 2009 है ।

(2) ये राजपत्र में प्रकाशन की तारीख को प्रवृत्त होंगे ।

2. **परिभाषाएं**. – इन नियमों में, जब तक संदर्भ से अन्यथा अपेक्षित न हो,–

(क) "अधिनियम" से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है ;

(ख) "संचार" से सूचना या संकेत का किसी रीति से प्रारूपण, पारेषण, वहन अभिप्रेत है और इसके अंतर्गत प्रत्यक्ष संचार और अप्रत्यक्ष संचार दोनों हैं ;

(ग) "संचार लिंक" से कंप्यूटर साधन के अंतः - संयोजन करने के लिए सेटेलाइट, माइक्रोवेव, रेडियो, टेरेस्ट्रियल लाइन, तार, बेतार या किसी अन्य संचार माध्यम का उपयोग अभिप्रेत है ;

(घ) "सक्षम प्राधिकारी" से संचार और सूचना प्रौद्योगिकी मंत्रालय के अधीन सूचना प्रौद्योगिकी विभाग में भारत सरकार का सचिव अभिप्रेत है ;

(ङ) "कंप्यूटर साधन" से अधिनियम की धारा 2 की उपधारा (1) के खंड (ट) में यथा परिभाषित कंप्यूटर साधन अभिप्रेत है ;

(च) "साइबर सुरक्षा घटना" से साइबर सुरक्षा के संबंध में कोई ऐसी वास्तविक या संदिग्ध प्रतिकूल घटना अभिप्रेत है जो लागू सुरक्षा नीति का प्रकट रूप से या अव्यक्त रूप से अतिक्रमण करती है, जिसका परिणाम सूचना का प्रसंस्करण या भंडारण या आंकड़ों में परिवर्तन के लिए किसी कंप्यूटर साधन तक अप्राधिकृत पहुंच, सेवा से इन्कार/व्यवधान, अप्राधिकृत प्रयोग प्राधिकार के बिना सूचना में होता है ;

(छ) "साइबर सुरक्षा भंग" से किसी व्यक्ति द्वारा आंकड़ों या सूचना का ऐसा अप्राधिकृत अर्जन या अप्राधिकृत प्रयोग अभिप्रेत है, जो किसी कंप्यूटर साधन में अनुरक्षित सूचना की गोपनीयता, अखंडता या उपलब्धता से समझौता करता है ;

(ज) "सूचना" से अधिनियम की धारा 2 की उपधारा (1) के खंड (v) में यथा परिभाषित सूचना अभिप्रेत है ,

(झ) "सूचना सुरक्षा पद्धतियों" से साइबर सुरक्षा घटनाओं और भंगों को कम करने के लिए सुरक्षा नीतियों और मानकों को लागू करना अभिप्रेत है ;

(ञ) "मध्यवर्ती" से अधिनियम की धारा 2 की उपधारा (1) के खंड (ध) में यथा परिभाषित कोई मध्यवर्ती अभिप्रेत है ,

(ट) "मानीटर" के अंतर्गत, उसके व्याकरणिक रूपभेदों और सजातीय पदों सहित, किसी मानीटर करनेवाली युक्ति के साधनों द्वारा किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त या भंडारित ट्रैफिक आंकड़ों या सूचना को देखना या उसका निरीक्षण करना या उसे अभिलिखित करना या संग्रह करना भी है ;

(ठ) "मानीटर करने वाली युक्ति" से कोई इलेक्ट्रोनिक, यांत्रिक, इलेक्ट्रो - यांत्रिक, इलेक्ट्रो चुम्बकीय, प्रकाशकीय या अन्य उपकरण, युक्ति, उपस्कर या साधित्र, जिसका या तो स्वयं या किसी अन्य उपकरण, युक्ति, उपस्कर या साधित्र के साथ संयोजन से, ट्रैफिक आंकड़ों या सूचना को देखने या निरीक्षण करने या अभिलिखित अथवा संग्रह करने के लिए उपयोग किया जाता है या उपयोग किया जा सकता है ;

(ड) "पोर्ट" या "उपयोजन पोर्ट" से ऐसे सॉफ्टवेयर नियमों का सैट अभिप्रेत है, जो उपयोजन से उपयोजन, नेटवर्क से नेटवर्क, कंप्यूटर से कंप्यूटर, कंप्यूटर प्रणाली से कंप्यूटर प्रणाली के बीच संचार का पता लगाता है और उसकी अनुज्ञा देता है ;

(ढ) "पुनर्विलोकन समिति" से भारतीय तार नियम, 1951 के नियम 419क के अधीन गठित पुनर्विलोकन समिति अभिप्रेत है ;

(ण) "सुरक्षा नीति" से सूचना और कंप्यूटर साधन का संरक्षण करने के लिए दस्तावेजीकृत कारबार नियम और प्रक्रियाएं अभिप्रेत हैं ;

(त) "ट्रैफिक आंकड़ों" से अधिनियम की धारा 69ख के स्पष्टीकरण (ii) में यथा परिभाषित ट्रैफिक आंकड़े अभिप्रेत हैं ;

3. मानीटर करने के लिए निदेश.– (1) अधिनियम की धारा 69ख की उपधारा (3) के अधीन ट्रैफिक आंकड़ों या सूचना के मानीटर करने और संग्रहण के लिए कोई निदेश, सक्षम प्राधिकारी द्वारा किए गए किसी आदेश के सिवाय, जारी नहीं किया जाएगा ।

(2) सक्षम प्राधिकारी साइबर सुरक्षा से संबंधित निम्नलिखित किसी या सभी प्रयोजनों के लिए मानीटर करने के निदेश जारी कर सकेगा, अर्थात :-

(क) आसन्न साइबर घटनाओं का पूर्वानुमान करना ;

(ख) कंप्यूटर साधन पर ट्रैफिक आंकड़ों या सूचना के साथ नेटवर्क उपयोजन का मानीटर करना ;

(ग) वायरसों या कंप्यूटर संदूषकों का पता लगाना और अवधारण करना ;

(घ) साइबर सुरक्षा भंगों या साइबर सुरक्षा घटनाओं को खोज निकालना;

(ङ) साइबर सुरक्षा भंग करने वाले या वायरस फैलाने वाले कंप्यूटर साधन या कंप्यूटर संदूषकों को खोज निकालना ;

(च) किसी ऐसे व्यक्ति की पहचान करना या उसे खोज निकालना, जिसने साइबर सुरक्षा को भंग किया है या जिसके बारे में भंग करने का संदेह है या जो भंग करने की संभावना के लिए संदिग्ध है ;

(छ) कंप्यूटर साधन में सूचना सुरक्षा प्रणालियों के अन्वेषण या आंतरिक संपरीक्षा के भाग रूप में संबंधित कंप्यूटर साधन की फॉरेंसिक के लिए उत्तरदायित्व ;

(ज) तत्समय प्रवृत्त साइबर सुरक्षा से संबंधित विधियों के किन्हीं उपबंधों के प्रवर्तन के लिए भंडारित सूचना तक पहुंच प्राप्त करना ;

(झ) साइबर सुरक्षा से संबंधित कोई अन्य विषय ।

(3) उपनियम (2) के अधीन सक्षम प्राधिकारी द्वारा जारी किए गए किसी निदेश में, ऐसे निदेश के लिए कारण अंतर्विष्ट होंगे और ऐसे निदेश की एक प्रति सात कार्यदिवसों की अवधि के भीतर पुनर्विलोकन समिति को अग्रेषित की जाएगी ।

(4) ट्रैफिक आंकड़ों या सूचना के मानीटर और संग्रह करने के लिए सक्षम प्राधिकारी के निदेश में किसी व्यक्ति या वर्ग के व्यक्तियों से या किसी विशिष्ट विषय से संबंधित ट्रैफिक आंकड़ों या सूचना का मानीटर और संग्रह करना सम्मिलित हो सकेगा, चाहे ऐसे ट्रैफिक आंकड़ों या सूचना या वर्ग के ट्रैफिक आंकड़ों या सूचना को एक या अधिक कंप्यूटर साधनों में प्राप्त किया जाता है, जो ऐसे कंप्यूटर साधन हैं जिनका एक विशिष्ट व्यक्ति या एक या बहुत परिसरों के सेट से या ट्रैफिक के लिए आंकड़ों या सूचना के जनन, पारेषण, प्राप्त, भंडारण करने के लिए उपयोग किए जाने की संभावना है ।

(4) ट्रैफिक आंकड़ों या सूचना के मानीटर या संग्रह करने के लिए सरकार का प्राधिकृत अभिकरण.- (1) सक्षम प्राधिकारी सरकार के किसी अभिकरण को किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त या भंडारित ट्रैफिक आंकड़ों या सूचना को मानीटर या संग्रह करने के लिए प्राधिकृत कर सकता है ।

(2) उप नियम (1) के अधीन सक्षम प्राधिकारी द्वारा प्राधिकृत अभिकरण एक या अधिक ऐसे नोडल अधिकारियों को, जो भारत सरकार के सचिव की पंक्ति से निम्न पंक्ति के न हों, नियम 3 के अधीन जारी किए गए निदेश को वहन करने वाली अध्यपेक्षा को प्राधिकृत करने और भेजने के प्रयोजन के लिए पदाभिहित करेगा ।

(3) उप नियम (2) के अधीन अध्यपेक्षा में उस अधिकारी या अभिकरण का नाम और पदाभिधान विनिर्दिष्ट होगा, जिसको मानीटर या संग्रह किए गए ट्रैफिक आंकड़ों या सूचना को प्रकट किया जाना है ।

(4) कंप्यूटर साधन के मध्यवर्ती या भारसाधक व्यक्ति एक या अधिक अधिकारियों को ट्रैफिक आंकड़ों या सूचना का मानीटर या संग्रह करने के लिए नोडल अधिकारी से ऐसी अध्यपेक्षा प्राप्त करने और ऐसी अध्यपेक्षा के संबंध में कार्रवाई करने के लिए पदाभिहित करेंगे ।

(5) मानीटर करने के लिए निदेश पहुंचाने वाली अध्यपेक्षा को कंप्यूटर साधन के मध्यवर्ती के पदाभिहित अधिकारियों या भारसाधक व्यक्ति को नोडल अधिकारी द्वारा लिखित पत्र या फैक्स द्वारा पहुंचाया जाएगा या ऐसे अधिकारी द्वारा, जो अवर सचिव की पंक्ति से निम्न पंक्ति का न हो या समतुल्य पंक्ति का हो, परिदत्त किया जाएगा (जिसके अंतर्गत इलेक्ट्रोनिक चिह्नांकन से चिह्नित ई-मेल द्वारा परिदान भी है) ।

(6) उपनियम (2) के अधीन मानीटर करने के लिए निदेश पहुंचाने वाली अध्यपेक्षा जारी करने वाला नोडल अधिकारी मध्यवर्ती के पदाभिहित अधिकारी या कंप्यूटर साधन के भारसाधक व्यक्ति को ऐसी अध्यपेक्षा में दर्शित स्वविधान के अनुसार मानीटर करने के लिए लिखित में भी अनुरोध करेगा और उसकी रिपोर्ट उपनियम (3) के अधीन पदाभिहित अधिकारी को करेगा ।

(7) नोडल अधिकारी उपस्कर के संस्थापन, हटाने और परीक्षण करने, सभी सुविधाएं, सहयोग और सहायता देने के लिए और ऑन लाइन पहुंच को भी समर्थ बनाने या ट्रैफिक आंकड़ों या सूचना का मानीटर और संग्रह करने के लिए कंप्यूटर साधन तक ऑन लाइन पहुंच को सुरक्षित करने और उसका उपबंध करने के लिए सभी सुविधाएं, सहयोग और सहायता देने के लिए उपनियम (4) के अधीन मध्यवर्ती के अधिकारी या कंप्यूटर साधन के भारसाधक व्यक्ति से भी अनुरोध करेगा ।

(8) नियम 3 के उपनियम (2) के अधीन जारी किए गए निदेश को पहुंचाने वाली उपनियम (2) के अधीन अध्यपेक्षा की प्राप्ति पर उपनियम (4) के अधीन मध्यवर्ती का पदाभिहित अधिकारी या कंप्यूटर साधन का भारसाधक व्यक्ति, पत्र या फैक्स या इलेक्ट्रोनिक रूप से चिह्नित ई-मेल के द्वारा अध्यपेक्षा की प्राप्ति की, नोडल अधिकारी को, ऐसी अध्यपेक्षा की प्राप्ति के समय से दो घंटे की अवधि के भीतर अभिस्वीकृति देगा ।

(9) उपनियम (4) के अधीन पदाभिहित मध्यवर्ती का अधिकारी या कंप्यूटर साधन का भारसाधक व्यक्ति उसके द्वारा प्राप्त की गई अध्यपेक्षाओं का उचित अभिलेख रखेगा ।

(10) मध्यवर्ती का पदाभिहित अधिकारी या कंप्यूटर साधन का भारसाधक व्यक्ति ट्रैफिक आंकड़ों या सूचना को मानीटर या संग्रह करने के लिए निदेश पहुंचाने वाली अध्यपेक्षा की एक सूची प्रत्येक पंद्रह दिन में नोडल अधिकारी को अग्रेषित करेगा, जिसमें संबंधित सक्षम प्राधिकारी के निदेश को पहुंचाने वाली अध्यपेक्षा के निर्देश और तारीख जैसे ब्यौरे सम्मिलित होंगे ।

5. मध्यवर्ती द्वारा ट्रैफिक आंकड़ों या सूचना के मानीटर या संग्रह करने के कार्य में प्रभावी नियंत्रण सुनिश्चित करना.— मध्यवर्ती या कंप्यूटर साधन का भारसाधक व्यक्ति उस स्थान पर यह सुनिश्चित करने के लिए पर्याप्त और प्रभावी आंतरिक नियंत्रण रखेगा कि ट्रैफिक आंकड़ों या सूचना को अप्राधिकृत रूप से मानीटर या संग्रह नहीं किया जाता है और अत्यधिक गोपनीयता रखी जाती है तथा ट्रैफिक आंकड़ों या सूचना के मानीटर या संग्रह करने के मामले में अत्यधिक सावधानी और पूर्वावधानी रखी जाती है क्योंकि उससे नागरिकों के निजीपन पर प्रभाव पड़ता है और यह भी कि इस मामले में मध्यवर्ती के पदाभिहित अधिकारी या कंप्यूटर साधन के भारसाधक व्यक्ति द्वारा ही कार्रवाई की जाती है ।

6. मध्यवर्ती का उत्तरदायित्व.— मध्यवर्ती या कंप्यूटर साधन का भारसाधक व्यक्ति अपने कर्मचारियों के कार्यों के लिए भी उत्तरदायी होंगे और सूचना की गोपनीयता और विश्वसनीयता को बनाए रखने या ट्रैफिक आंकड़ों या सूचना के अप्राधिकृत रूप से मानीटर या संग्रह करने से संबंधित अधिनियम और उसके अधीन बनाए गए नियमों के उपबंधों के अतिक्रमण के मामले में मध्यवर्ती या कंप्यूटर साधन का भारसाधक व्यक्ति तत्समय प्रवृत्त विधियों के सुसंगत उपबंध के अधीन किसी कार्रवाई के लिए दायी होगा ।

7. सक्षम प्राधिकारी के निदेशों का पुनर्विलोकन.— पुनर्विलोकन समिति की बैठक दो मास में कम से कम एक बार होगी और समिति अपने उन निष्कर्षों को अभिलिखित करेगी कि क्या नियम 3 के उपनियम (2) के अधीन जारी किए गए निदेश अधिनियम की धारा 69ख की उपधारा (3) के उपबंधों के अनुसार हैं और जहां पुनर्विलोकन समिति की यह राय है कि निदेश उक्त निर्दिष्ट उपबंधों के अनुसार नहीं है, वहां वह निदेशों को अपास्त कर सकेगी और प्रतियों के, जिनके अंतर्गत मानीटर या संग्रह किए गए ट्रैफिक आंकड़ों या सूचना का तत्संबंधी इलेक्ट्रोनिक अभिलेख भी हैं, नष्ट करने के लिए आदेश जारी कर सकेगी ।

8. अभिलेखों को नष्ट करना.– (1) प्रत्येक अभिलेख, जिसके अंतर्गत ट्रैफिक आकड़ों का मानीटर या संग्रह करने के लिए ऐसे निदेशों से संबंधित इलेक्ट्रोनिक अभिलेख भी है, निदेश की प्राप्ति या अभिलेख के सृजन से, जो भी पश्चात्वर्ती हो, नौ मास की अवधि की समाप्ति के पश्चात, सिवाए उस दशा के जहां ट्रैफिक आंकड़े या सूचना कृत्यकारी अपेक्षाओं के लिए अपेक्षित है या होने की संभावना है, नष्ट कर दिया जाएगा ।

(2) किसी चल रहे अन्वेषण, आपराधिक परिवाद या विधिक कार्यवाहियों के प्रयोजन के लिए अपेक्षित से अन्यथा के सिवाय मध्यवर्ती कंप्यूटर साधन का भारसाधक व्यक्ति सूचना के मानीटर करने या संग्रह के निदेशों से संबंधित अभिलेखों को, ट्रैफिक आंकड़ों का मानीटर करना या संग्रह बंद किए जाने के छह मास की अवधि के भीतर, नष्ट करेगा ।

9. प्राधिकार के बिना ट्रैफिक आंकड़ों या सूचना को मानीटर या संग्रह करने का प्रतिषेध.– (1) कोई व्यक्ति, जो साशय या जानबूझकर, नियम 3 के उपनियम (2) या नियम 4 के उपनियम (1) के अधीन प्राधिकार के बिना ट्रैफिक आंकड़ों या सूचना का भारत के भीतर किसी स्थान पर उसके होने या पारेषण के अनुक्रम में मानीटर या संग्रह करता है या ट्रैफिक आंकड़ों या सूचना का मानीटर करने या संग्रह करने का प्रयास करता है या ट्रैफिक आंकड़ों या सूचना का मानीटर या संग्रह करने के लिए किसी व्यक्ति को प्राधिकृत करता है या उसकी सहायता करता है, उसके विरुद्ध कार्यवाही की जाएगी उसे तत्समय प्रवृत्त विधि के सुसंगत उपबंधों के अधीन तदनुसार दंडित किया जाएगा ।

(2) कंप्यूटर साधन में ट्रैफिक आंकड़ों या सूचना का किसी मध्यवर्ती के कर्मचारी या कंप्यूटर साधन के भारसाधक व्यक्ति द्वारा या मध्यवर्ती द्वारा सम्यक रूप से प्राधिकृत व्यक्ति द्वारा मानीटर या संग्रह उस मध्यवर्ती द्वारा प्रदाय की गई सेवाओं से संबंधित उसके कर्तव्य के अनुक्रम में किया जा सकेगा, यदि ऐसे कार्यकलाप प्रवृत्त उद्योग पद्धतियों के अनुसार उसके कर्तव्यों के निर्वहन के लिए निम्नलिखित मामलों के संबंध में युक्तियुक्त रूप से आवश्यक हैं :-

(i) कंप्यूटर साधन का या कंप्यूटर साधन के साथ प्रयोग किए जाने वाले किसी उपस्कर का संस्थापन ;

(ii) कंप्यूटर साधन का प्रचालन या अनुरक्षण ; या

(iii) मध्यवर्ती या अभिदाता के सिरे पर किसी संचार लिंक या सॉफ्टवेयर का संस्थापन या मध्यवर्ती के कंप्यूटर साधन पर उपयोगकर्ता लेखा का संस्थापन और उसकी कृत्यकारिता के लिए उसका परीक्षण ;

(iv) उपस्कर, कंप्यूटर साधन या किसी संचार लिंक या कोड के संस्थापन, संयोजन या अनुरक्षण से संबंधित कंप्यूटर साधन से भंडारित सूचना तक पहुंच प्राप्त करना ; या

(v) कंप्यूटर साधन से निम्नलिखित प्रयोजन के लिए भंडारित सूचना तक पहुंच प्राप्त करना :

(क) कंप्यूटर साधन में सूचना सुरक्षा पद्धतियों का कार्यान्वयन ;

(ख) सुरक्षा भंगों, कंप्यूटर संदूषकों या कंप्यूटर वायरस का अवधारण करना ;

(ग) अन्वेषण या आंतरिक संपरीक्षा के भाग रूप में संबंधित कंप्यूटर साधन की फॉरेंसिक का उत्तरदायित्व लेना ; या

(vi) कंप्यूटर साधन या किसी व्यक्ति को, जिसने अधिनियम के किसी उपबंध का उल्लंघन किया है या जिसके बारे में उल्लंघन करने का संदेह है या जो उल्लंघन करने के लिए संभाव्य है, जिसकी मध्यवर्ती द्वारा प्रदाय की गई सेवाओं पर प्रतिकूल प्रभाव पड़ने की संभावना है, खोजने के प्रयोजन के लिए कंप्यूटर साधन से सूचना तक पहुंचना या उसका विश्लेषण करना ।

(3) मध्यवर्ती या कंप्यूटर साधन का भारसाधक व्यक्ति और उसके कर्मचारी उपनियम (2) के अधीन यथाविनिर्दिष्ट कार्यों का पालन करते हुए कड़ी गोपनीयता और विश्वसनीयता रखेगा ।

(4) मानीटर किए गए या संग्रहित ट्रैफिक आंकड़ों या सूचना के ब्यौरों का मध्यवर्ती या कंप्यूटर साधन के भारसाधक व्यक्ति या उसके किसी कर्मचारी द्वारा उपयोग नहीं किया जाएगा या उसे नियम 4 के उपनियम (2) के अधीन उक्त सूचना के आशयित प्राप्तकर्ता से भिन्न किसी व्यक्ति को प्रकट नहीं किया जाएगा । किसी मध्यवर्ती या उसके कर्मचारी या कंप्यूटर साधन के भारसाधक व्यक्ति के विरुद्ध, जो इस नियम के उपबंधों का उल्लंघन करता है, कार्रवाई की जाएगी और उसे इस अधिनियम या तत्समय प्रवृत्त किसी अन्य विधि के सुसंगत उपबंधों के अधीन तदनुसार दंडित किया जाएगा ।

10. प्राधिकृत अभिकरण द्वारा ट्रैफिक आंकड़ों के या सूचना के प्रकट करने का प्रतिषेध.— मानीटर किए गए या संग्रहित ट्रैफिक आंकड़ों या सूचना के ब्यौरों का नियम 4 के उपनियम (1) के अधीन प्राधिकृत अभिकरण द्वारा किसी अन्य प्रयोजन के लिए, आसन्न साइबर खतरों या इंटरनेट पर पोर्ट - अनुसार ट्रैफिक के साधारण रुझानों का पूर्वानुमान लगाने या साइबर घटनाओं के साधारण विश्लेषण या अन्वेषण के लिए अथवा भारत में सक्षम न्यायालय के समक्ष न्यायिक कार्यवाहियों में के सिवाय, उपयोग नहीं किया जाएगा या उसे प्रकट नहीं किया जाएगा ।

11. विश्वसनीयता का बनाए रखा जाना—नियम 10 में यथा अन्यथा उपबंधित के सिवाए इन नियमों के अधीन सक्षम प्राधिकारी द्वारा जारी किए गए ट्रैफिक आंकड़ों या सूचना को मानीटर करने या संग्रह करने के लिए निदेशों के संबंध में कड़ी गोपनीयता रखी जाएगी ।

[सं. 9(16)/2004 ई.सी.]

एन. रवि शंकर, संयुक्त सचिव

NOTIFICATION

New Delhi, the 27th October, 2009

G.S.R. 782 (E).— In exercise of the powers conferred by clause (za) of sub-section (2) of section 87, read with sub-section (3) of section 69B of the Information Technology Act 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:—

1. **Short title and commencement.**— (1) These rules may be called the Information Technology (Procedure and safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. **Definitions.**— In these rules, unless the context otherwise requires,—

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "communication" means dissemination, transmission, carriage of information or signal in some manner and include both a direct communication and an indirect communication;

(c) "communication link" means the use of satellite, microwave, radio, terrestrial line, wire, wireless or any other communication media to inter-connect computer resource;

(d) "competent authority" means the Secretary to the Government of India in the Department of Information Technology under the Ministry of Communications and Information Technology;

(e) "computer resource" means computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;

(f) "cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service/ disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(g) "cyber security breaches" means unauthorised acquisition or unauthorised use by a person of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource;

(h) "information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(i) "information security practices" means implementation of security policies and standards in order to minimize the cyber security incidents and breaches;

(j) "intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

(k) "monitor" with its grammatical variations and cognate expressions, includes to view or inspect or record or collect traffic data or information generated, transmitted, received or stored in a computer resource by means of a monitoring device;

(l) "monitoring device" means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself in combination with any other instrument, device, equipment or apparatus, to view or inspect or record or collect traffic data or information;

(m) "port" or "application port" means a set of software rules which identifies and permits communication between application to application, network to network, computer to computer, computer system to computer system;

(n) "Review Committee" means the Review Committee constituted under rule 419A of the Indian Telegraph Rules, 1951;

(o) "security policy" means documented business rules and processes for protecting information and the computer resource;

(p) "traffic data" means traffic data as defined in *Explanation (ii)* to section 69B of the Act.

3. **Directions for monitoring** — (1) No directions for monitoring and collection of traffic data or information under sub-section (3) of section 69B of the Act shall be issued, except by an order made by the competent authority.

(2) The competent authority may issue directions for monitoring for any or all of the following purposes related to cyber security, namely:-

(a) forecasting of imminent cyber incidents;

(b) monitoring network application with traffic data or information on computer resource;

(c) identification and determination of viruses or computer contaminant;

(d) tracking cyber security breaches or cyber security incidents;

(e) tracking computer resource breaching cyber security or spreading virus or computer contaminants;

(f) identifying or tracking of any person who has breached, or is suspected of having breached or being likely to breach cyber security;

(g) undertaking forensic of the concerned computer resource as a part of investigation or internal audit of information security practices in the computer resource;

(h) accessing a stored information for enforcement of any provisions of the laws relating to cyber security for the time being in force;

(i) any other matter relating to cyber security.

(3) Any direction issued by the competent authority under sub-rule (2) shall contain reasons for such direction and a copy of such direction shall be forwarded to the Review Committee within a period of seven working days.

(4) The direction of the competent authority for monitoring and collection of traffic data or information may include the monitoring and collection of traffic data or information from any person or class of persons or relating to any particular subject whether such traffic data or information, or class of traffic data or information, are received with one or more computer resources, being a computer resource likely to be used for the generation, transmission, receiving, storing of traffic data or information from or to one particular person or one or many set of premises.

4. **Authorised agency of Government for monitoring and collection of traffic data or information** — (1) The competent authority may authorise any agency of the government for monitoring and collection of traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The agency authorised by the competent authority under sub-rule (1) shall designate one or more nodal officer, not below the rank of the Deputy Secretary to the Government of India, for the purpose to authenticate and send the requisition conveying direction issued under rule 3 to the designated officers of the concerned intermediary or person in-charge of computer resources.

(3) The requisition under sub-rule (2) shall specify the name and designation of the officer or the agency to whom the monitored or collected traffic data or information is to be disclosed.

(4) The intermediaries or person in-charge of computer resource shall designate one or more officers to receive requisition and to handle such requisition from the nodal officer for monitoring or collection of traffic data or information.

(5) The requisition conveying directions for monitoring shall be conveyed to the designated officers of the intermediary or person in-charge of computer resources, in writing through letter or fax by the nodal officer or delivered, (including delivery by email signed with electronic signature), by an officer not below the rank of Under Secretary or officer of the equivalent rank.

(6) The nodal officer issuing the requisition conveying directions for monitoring under sub-rule (2) shall also make a request in writing to the designated officer of intermediary or person in-charge of computer resource for monitoring in accordance with the format indicated in such requisition and report the same to the officer designated under sub-rule (3).

(7) The nodal officer shall also make a request to the officer of intermediary or person in-charge of computer resource designated under sub-rule (4) to extend all facilities, co-operation and assistance in installation, removal and testing of equipment and also enable online access or to secure and provide online access to the computer resource for monitoring and collecting traffic data or information.

(8) On receipt of requisition under sub-rule (2) conveying the direction issued under sub-rule (2) of rule 3, the designated officer of the intermediary or person in-charge of computer resource designated under sub-rule (4) shall acknowledge the receipt of requisition by way of letter or fax or electronically signed e-mail to the nodal officer within a period of two hours from the time of receipt of such requisition.

(9) The officer of the intermediary or person in-charge of computer resource designated under sub-rule (4) shall maintain proper records of the requisitions received by him.

(10) The designated officer of the intermediary or person in-charge of computer resource shall forward in every fifteen days a list of requisition conveying direction for monitoring or collection of traffic data or information to the nodal officer which shall include details such as the reference and date of requisition conveying direction of the concerned competent authority.

5. **Intermediary to ensure effective check in handling monitoring or collection of traffic data or information.**— The intermediary or person in-charge of computer resources shall put in place adequate and effective internal checks to ensure that unauthorised monitoring or collection of traffic data or information does not take place and extreme secrecy is maintained and utmost care and precaution is taken in the matter of monitoring or collection of traffic data or information as it affects privacy of citizens and also that this matter is handled only by the designated officer of the intermediary or person in-charge of computer resource.

6. **Responsibility of intermediary.**— The intermediary or person in-charge of computer resource shall be responsible for the actions of their employees also, and in case of violation of the provision of the Act and rules made thereunder pertaining to maintenance of secrecy and confidentiality of information or any unauthorised monitoring or collection of traffic data or information, the intermediary or person in-charge of computer resource shall be liable for any action under the relevant provision of the laws for the time being in force.

7. **Review of directions of competent authority.**— The Review Committee shall meet at least once in two months and record its findings whether the directions issued under sub-rule (2) of rule 3 are in accordance with the provisions of sub-section (3) of section 69B of the Act and where the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and issue order for destruction of the copies, including corresponding electronic record of the monitored or collected traffic data or information.

8. **Destruction of records.**— (1) Every record, including electronic records pertaining to such directions for monitoring or collection of traffic data shall be destroyed by the designated officer after the expiry of a period of nine months from the receipt of direction or creation of record, whichever is later, except in a case where the traffic data or information is, or likely to be, required for functional requirements.

(2) Save as otherwise required for the purpose of any ongoing investigation, criminal complaint or legal proceedings the intermediary or the person in-charge of computer resource shall destroy records pertaining to directions for monitoring or collection of information within a period of six months of discontinuance of the monitoring or collection of traffic data and in doing so they shall maintain extreme secrecy.

9. **Prohibition of monitoring or collection of traffic data or information without authorisation.**— (1) Any person who, intentionally or knowingly, without authorisation under sub-rule (2) of rule 3 or sub-rule (1) of rule 4, monitors or collects traffic data or information, or attempts to monitor or collect traffic data or information, or authorises or assists any person to monitor or collect traffic data or information in the course of its occurrence or transmission at any place within India, shall be proceeded against, punished accordingly under the relevant provisions of the law for the time being in force

(2) The monitoring or collection of traffic data or information in computer resource by the employee of an intermediary or person in-charge of computer resource or a person duly authorised by the intermediary, may be undertaken in course of his duty relating to the services provided by that intermediary, if such activities are reasonably necessary for the discharge his duties as per the prevailing industry practices, in connection with the following matters, namely :—

(i) installation of computer resource or any equipment to be used with computer resource; or
(ii) operation or maintenance of computer resource, or
(iii) installation of any communication link or software either at the end of the intermediary or subscriber, or installation of user account on the computer resource of intermediary and testing of the same for its functionality;
(iv) accessing stored information from computer resource relating to the installation, connection or maintenance of equipment, computer resource or a communication link or code; or
(v) accessing stored information from computer resource for the purpose of —
  (a) implementing information security practices in the computer resource,
  (b) determining any security breaches, computer contaminant or computer virus,
  (c) undertaking forensic of the concerned computer resource as a part of investigation or internal audit; or
(vi) accessing or analysing information from a computer resource for the purpose of tracing a computer resource or any person who has contravened, or is suspected of having contravened or being likely to contravene, any provision of the Act that is likely to have an adverse impact on the services provided by the intermediary.

(3) The intermediary or the person in-charge of computer resource and its employees shall maintain strict secrecy and confidentiality of information while performing the actions as specified under sub-rule (2).

(4) The details of monitored or collected traffic data or information shall not be used or disclosed by intermediary or person in-charge of computer resource or any of its employees to any person other than the intended recipient of the said information under sub-rule (2) of rule 4. Any intermediary or its employees or person in-charge of computer resource who contravenes the provisions of this rule shall be proceeded against and punished accordingly under the relevant provisions of the Act or any other law for the time being in force.

10. **Prohibition of disclosure of traffic data or information by authorised agency.**— The details of monitored or collected traffic data or information shall not be used or disclosed by the agency authorised under sub-rule (1) of rule 4 for any other purpose, except for forecasting imminent cyber threats or general trend of port-wise traffic on Internet, or general analysis of cyber incidents, or for investigation or in judicial proceedings before the competent court in India.

11. **Maintenance of confidentiality.**— Save as otherwise provided in rule 10, strict confidentiality shall be maintained in respect of directions for monitoring or collection of traffic data or information issued by the competent authority under these rules.

[No. 9(16)/2004-EC]
N. RAVI SHANKER, Jt. Secy.

Printed by the Manager, Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.