सर्वोच्च प्राथमिकता

ओ0पी0 सिंह

डीजी परिपत्र संख्या-22/2018

पुलिस महानिदेशक,
उत्तर प्रदेश
1 तिलक मार्ग, लखनऊ।
दिनांक : लखनऊ : मई 13 ,2018

प्रिय महोदय,

गृह मंत्रालय, भारत सरकार ने अपने परिपत्र संख्या-24013/31/2015-CSR-IV/CIS दिनांक 13.01.2018 के माध्यम से साइबर क्राइम की रोकथाम और नियंत्रण के सम्बन्ध में एक एडवाइजरी जारी की है जिसमें समग्रतापूर्वक पूरी विषयवस्तु पर दिशा-निर्देश सम्मिलित हैं। उल्लेखनीय है कि विभिन्न प्रकार के साइबर अपराधों यथा वेबसाइट डिफेसमेन्ट, ऑनलाइन फाइनेन्सियल फ्राड, ऑन लाइन स्टाकिंग/हेरेसमेन्ट, डोमेन थेफ्ट/डाटा थेफ्ट, सोशल मीडिया पर आपराधिक गतिविधियाँ आदि के लिए विशिष्ट विवेचनात्मक दक्षता और फोरेन्सिक टूल की आवश्यकता पड़ती है। इस प्रक्रिया में तकनीकी, प्रशासनिक और कानूनी चुनौतियों के दृष्टिगत रखते हुये पूर्व में इस विषय से सम्बन्धित डी0जी0 परिपत्र संख्या-01/2016 दिनांक 8.1.2016, डी0जी0परिपत्र संख्या-17/2016 दिनांक 16.3.16, डी0जी0 परिपत्र संख्या 06/2017 दिनांक 26.3.17 एवं डी0जी0 परिपत्र संख्या 08/2017 दिनांक 28.03.2017 को सम्मिलित कर गृह मंत्रालय के संदर्भित एडवाइजरी के अनुरूप समस्त बिन्दुओं को सम्मिलित करते हुए पुनः निम्न व्यवस्था एवं निर्देश निर्गत किये जा रहे हैं:-

राज्य साइबर समन्वय सेल:-

उत्तर प्रदेश पुलिस के अन्तर्गत 'राज्य साइबर क्राइम समन्वय (Coordination) सेल' पुलिस महानिरीक्षक एस0टी0एफ0 के नेतृत्व में गठित किया गया है जिन्हें 'राज्य साइबर क्राइम समन्वयक' कहा जायेगा। यह सेल जनपदीय स्तर पर स्थापित साइबर क्राइम सेल के प्रशिक्षण, विवेचना में मार्ग दर्शन, एवं अन्तर्राज्यीय समन्वय के लिए उत्तरदायी होगा। यह सेल उत्तर प्रदेश पुलिस के भिज्ञ अधिकारियों/कर्मियों को को-आप्ट करने तथा आवश्यकतानुसार साइबर सिक्योरिटी विशेषज्ञों को आऊटसोर्सिंग के माध्यम अनुबन्धित करने के लिए स्वतंत्र होगा।

जनपद साइबर सेल:-

प्रत्येक जनपद में अपर पुलिस अधीक्षक, अपराध/पुलिस उपाधीक्षक, अपराध के नेतृत्व में 'जनपदीय साइबर सेल' गठित किया जायेगा जिसमें पर्याप्त संख्या में निरीक्षक/उप-निरीक्षक तथा अन्य कर्मी नियुक्त होंगे। यह वर्तमान में गठित काइम ब्रांच का हिस्सा होगा तथा यह सेल जनपदीय पुलिस अधीक्षक के अधीन कार्य करेगा और राज्य साइबर समन्वय सेल से विवचेना के सम्बन्ध में निर्देश प्राप्त करेगा।

सोशल मीडिया: निगरानी और कार्यवाही:-

वर्तमान समय में विचारों और सूचनाओं के आदान-प्रदान में सोशल मीडिया की महत्वपूर्ण भूमिका हो गई है। इसकी व्यापकता और शीघ्रता से लोगों तक पहुँचने की क्षमता के कारण इसका दुरूपयोग धार्मिक उन्माद फैलाने, दूसरे धर्म के प्रति लोगों में द्वेष पैदा करने, व्यक्तिगत प्रतिष्ठा में ठेस पहुँचाने, अश्लील विडियो अपलोड करने और महिलाओं/युवतियों को ब्लैकमेल करने जैसे आपराधिक कृत्यों के लिए भी किया जा रहा है। इसके कारण कानून व्यवस्था सम्बन्धी गम्भीर समस्यायें उत्पन्न हो जाती हैं। सामान्य रूप से इनके लिए Facebook, Twitter, WhatsApp, Youtube, Instagram, Google+ आदि सेवाओं का प्रयोग किया जा रहा है।

a) निगरानी:- सोशल मीडिया पर की जा रही टिप्पणी और उसकी प्रतिक्रिया की सतत् निगरानी हेतु समस्त रेंज कार्यालयों को Advance Application Social Media Analytics (AASMA) का एक्सेस दिया गया है। एक्सेस करने हेतु IP address: http://117.247.255.218:3389 पर टाइप कर Login करना होता है। सभी रेंजों के Login ID एवं Password (संलग्नक:A) में उपलब्ध हैं।

b) कार्यवाही:-

i) **Blocking on Indian ISPs** (बन्द करना)- आपत्तिजनक एवं भड़काऊ Page/Profile/Post/Tweet/Video आदि चिन्हित होने पर भारत में उनका Public Access तत्काल Block करने हेतु दूरसंचार एवं सूचना प्राद्यौगिकी मंत्रालय भारत सरकार के परिपत्र संख्या-GSR 781(E) दिनांक 27.10.2009

के अनुसार कार्यवाही करनी होगी। परिपत्र के प्राविधानों के अन्तर्गत उत्तर प्रदेश में विशेष सचिव, सूचना प्राद्यौगिकी नोडल आफिसर हैं। अतः किसी Facebook, Twitter, WhatsApp, Youtube, Instagram, Google+ आदि साइट्स को Block करने हेतु परिपत्र में दिये गये फार्म 6(2) को भरकर जनपदीय पुलिस अधीक्षक द्वारा मोहर एवं हस्ताक्षर कराकर उसकी PDF फाइल बनाकर हार्डकापी सहित राज्य नोडल अधिकारी के माध्यम से डेजिग्नेटेड आफिसर/ग्रुप कोआर्डिनेटर को निम्नलिखित पते/ई-मेल पर भेजें।

Group Coordinator
Cyber Law Division
Department of Electronics &
Information Technology,
6, C.G.O., Complex, Lodhi Road
New Delhi-110003/

E-mail ID- Cyberlaw@meity.gov.in,
gccyberlaws@ meity.gov.in

ii) सोशल नेटवर्किंग साइट पर **Facebook, Twitter, WhatsApp, Youtube, Instagram, Google+** आदि साइट्स को **Block** करने तथा उक्त प्रकार के कन्टेन्ट को पोस्ट/अपलोड करने वाले की जानकारी प्राप्त करने हेतु कार्यवाही:-

a) सम्बन्धित कन्टेन्ट का URL Address Bar से Copy कर लिया जाय।

b) आपत्तिजनक कन्टेन्ट का स्क्रीनशॉट ले लिया जाय।

c) आपत्तिजनक कन्टेन्ट को पोस्ट/अपलोड करने वाले संदिग्ध की पहचान हेतु सम्बन्धित सोशल नेटवर्किंग साइट के नोडल डेस्क को धारा-91 दं0प्र0सं0 के अन्तर्गत राजपत्रित अधिकारी के हस्ताक्षर एवं मुहरयुक्त PDF फार्मेट में अंग्रेजी में ई-मेल भेजा जाय।

d) धारा-91 द0प्र0सं0 नोटिस में आवश्यकतानुसार Creation IP Address/Data/Time(Time Zone सहित) तथा किसी विशिष्ट Post, Massage, Tweet,Video आदि के लिए अपलोड करने वाले के IP Address/Data/Time (Time Zone सहित) प्राप्त किया जाय।

e) Social Media Sites से सूचना प्राप्त करने एवं Block करने हेतु निम्न E-mail ID पर E-mail किया जाय:-

Social Networking Sites	E-mail ID
TWITTER	tw-le-requests@twitter.com
FACEBOOK	records@fb.com
YOUTUBE	lis-apac@google.com
GOOGLE+	lis-apac@google.com
INSTAGRAM	इस Site पर Abuse Report सीधे Website पर उपलब्ध Form भरकर प्रेषित की जा सकती है।
FLICKR	इस Site पर आपत्तिजनक विषयवस्तु के सम्बन्ध में Abuse Report प्रेषित करनी होगी।

f) संदिग्ध का IP address, date, time प्राप्त होने पर सर्वप्रथम दिए गए time को IST में परिवर्तित किया जाय और फिर IP address के आधार पर चिन्हित ISP (Internet Service Provider) से संदिग्ध के सम्बन्ध में सुसंगत सूचनायें प्राप्त कर कार्यवाही की जाए।

g) उक्त सभी ई-मेल NIC पर बनी mail ID से ही भेजी जाय।

h) यदि किसी गम्भीर प्रकरण की विवेचना के मध्य सोशल मीडिया साइट से प्राप्त डाटा का उपयोग साक्ष्य के लिए करना हो तो स्थापति प्रक्रिया के अनुसार Mutual Legal Assistant Treaty (MLAT) के अन्तर्गत सम्बन्धित माननीय न्यायालय से Letter Rogatary (LR) प्राप्त कर CBI स्थित International Police Coopration Cell (IPCC) के माध्यम से

डाटा पुनः प्राप्त किया जायेगा। IPCC का सम्पर्क सूत्र निम्नलिखित है:-

Assistant Director, IPCC,
Office of CBI
Plot No 5-B, CGO Complex,
Lodhi Road, New Delhi-110003EPABX Board Nos: 011-24360422/24360276

iii) प्रथम सूचना रिपोर्ट का पंजीकरण:-

पीड़ित द्वारा प्राप्त सूचना का विश्लेषण कर आई0टी0 एक्ट एवं भा0दं0वि0 की सुसंगत धाराओं में प्रथम सूचना रिपोर्ट पंजीकृत कराई जायेगी। प्रायः जनपदों में आई0टी0 की धाराओं के प्रयोग के सम्बन्ध में भ्रम की स्थिति बनी रहती है इसलिये परिपत्र के साथ विभिन्न प्रकार के अपराधों में आकृष्ट होने वाली आई0टी0 एक्ट अथवा भा0दं0वि0 की धाराओं का उल्लेख करते हुये एक तालिका संलग्न की जा रही है। (संलग्नक:B)

iv) विवेचना के मध्य डिजिटल साक्ष्य प्राप्त करने हेतु बरामद कम्प्यूटर, लैपटॉप, मोबाइल, पेनड्राइव, हार्डडिस्क आदि इलेक्ट्रानिक डिवाइसों का फोरेन्सिक परीक्षण कराने की आवश्यकता रहती है। प्रायः देखा जा रहा है कि विवेचकों द्वारा इस महत्वपूर्ण साक्ष्य के संकलन हेतु पर्याप्त प्रयास नहीं किये जा रहे हैं। जिन विवेचकों अथवा पर्यवेक्षक अधिकारियों द्वारा इस दिशा में पहल की भी जाती है उनमें FSL से मांगे जाने वाली सूचनाओं में स्पष्टता नहीं होती है। अतः यह सुनिश्चित कराया जाय कि FSL, महानगर, लखनऊ में डिजिटल साक्ष्य प्राप्त करने के लिए भेजे जाने वाले उपकरणों के साथ पूर्व निर्धारित प्रपत्र में सम्बन्धित केस के अनुसार प्रश्न अवश्य पूछे जायें।

मै आपसे अपेक्षा करता हूँ कि उक्त निर्देशों का भलीभाँति अध्ययन करके कार्यशाला के माध्यम से समस्त अधीनस्थों को भी अवगत करायें। यह सुनिश्चित किया जाय कि साइबर स्पेस में होने वाले अपराधों और इंटरनेट के माध्यम से समाज में साम्प्रदायिकता, आपत्तिजनक एवं भ्रामक सूचना फैलाने वालों के विरूद्ध त्वरित वैधानिक कार्यवाही हो सके एवं समाज विरोधी गतिविधियों पर अंकुश लगाने के लिए समय से विधिसम्मत कार्यवाही की जा सके।

सभी उपरोक्त निर्देशों का कड़ाई से अनुपालन सुनिश्चित करेंगे।

संलग्नक-यथोपरि।

भवदीय,

13.5.18

(ओ0पी0 सिंह)

समस्त जोनल अपर पुलिस महानिदेशक,
उत्तर प्रदेश।
समस्त परिक्षेत्रीय पुलिस महानिरीक्षक/पुलिस उपमहानिरीक्षक,
उत्तर प्रदेश।
समस्त वरिष्ठ पुलिस अधीक्षक/पुलिस अधीक्षक (नाम से)
जनपद/रेलवे, उत्तर प्रदेश।

प्रतिलिपि-निम्न को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित:-

1. अपर पुलिस महानिदेशक, रेलवे, उ0प्र0।
2. अपर पुलिस महानिदेशक, तकनीकी सेवाएं, उ0प्र0।
3. पुलिस महानिरीक्षक, ए0टी0एस0, एस0टी0एफ0, उ0प्र0।
4. समस्त राजपत्रित अधिकारी, मुख्यालय पुलिस महानिदेशक, उ0प्र0।

संलग्नक–A (AASMA) से सम्बन्धित लॉगिन आई0डी0 एवं पासवर्ड की सूची

Login ID of all Ranges:

Sl.No.	Loging ID	Password
1	agrarange@aasma.com	agrarange
2	aligarhrange@aasma.com	aligarhrange
3	allahabadrange@aasma.com	allahabadrange
4	chitrakootdhamrange@aasma.com	chitrakootdhamrange
5	moradabadrange@aasma.com	moradabadrange
6	bareillyrange@aasma.com	bareillyrange
7	devipatanrange@aasma.com	devipatanrange
8	bastirange@aasma.com	bastirange
9	gorakhpurrange@aasma.com	gorakhpurrange
10	kanpurrange@aasma.com	kanpurrange
11	jhansirange@aasma.com	jhansirange
12	lucknowrange@aasma.com	lucknowrange
13	faizabadrange@aasma.com	faizabadrange
14	saharanpurrange@aasma.com	saharanpurrange
15	azamgarhrange@aasma.com	azamgarhrange
16	varanasirange@aasma.com	varanasirange
17	mirzapurrange@aasma.com	mirzapurrange

Distt of Meerut Range

Sl.No.	Loging ID	Password
1	disttmeerut@aasma.com	disttmeerut
2	distthapur@aasma.com	distthapur
3	disttghaziabad@aasma.com	disttghaziabad
4	disttbaghpat@aasma.com	disttbaghpat
5	disttgoutambuddhanagar@aasma.com	disttgoutambuddhanagar
6	disttbulandshahr@aasma.com	disttbulandshahr

संलग्नक—B

Sr. No.	NATURE OF COMPLAINT	APPLICABLE SECTIONS UNDER IT ACT 2008	APPLICABLE SECTION UNDER OTHER LAWS
1	Promotion of disharmony, enmity or feelings of hatred		Sec 153A IPC
2	Statements conducting public mischief		Sec 505(2) IPC
3	deliberate and malicious acts intended to outrage the religious feelings of any class by insulating its religion		Sec 295 A IPC
4	Mobile phone lost/stolen	-	Sec 379 IPC
5	Receiving stolen computer/mobile phone/data	Sec 66 B 3 years imprisonment or Rs 1 lakh fine or both	Sec 411 IPC
6	A password is stolen and used by fraudulent purpose	Sec 66 C 3 years imprisonment or Rs 1 lakh fine or both	Sec 419 Sec 420
7	An email is read by someone else by fraudulently making use of password	Sec 66 3 years imprisonment or Rs 3 lakh fine or both	Sec 66
8	A biometric thumb impression is misused	Sec 66 C 3 years imprisonment or Rs 1 lakh fine or both	
9	An electronic signature or digital signature is misused	Sec 66 C 3 years imprisonment or Rs 1 lakh fine or both	
10	A phishing e-mail is sent out in your name, asking for login credentials	Sec 66 D 3 years imprisonment or Rs 1 lakh fine or both	Sec 419 IPC
11	Capturing publishing, or transmitting the image of the private part without any person's consent or knowledge	Sec 66 E 3 years imprisonment or Rs 2 lakh fine or both	Sec 292 IPC
12	Tampering with computer source documents	Sec 65 3 years' imprisonment or Rs 2 lakh fine or both	
13	Data modification	Sec 66 3 years' imprisonment or Rs 5 lakh fine or both	
14	Sending offensive messages through communication service	Sec 66 3 years' imprisonment	Sec 500 / 504/ 506 IPC
15	Publishing or transmitting obscene material in	Sec 67 3 years' imprisonment and up to 10 lakh fine	Sec 292 IPC
16	Publishing or transmitting of material containing sexually explicit act in electronic form	Sec 67A 5 years' imprisonment and up to 10 lakh fine	Sec 292 IPC

17	**Misusing a Wi-Fi connection for acting against the state**	**Sec 66** 3 years' imprisonment or Rs 5 lakh fine or both	
18	**Conducting a denial of service attack against a government computer**	**Sec 66** 3 years' imprisonment or Rs 5 lakh fine or both **66F** life imprisonment	
19	**Not allowing the authorities to decrypt all communication that passes through your computer or network**	**Sec 69** 7 years' imprisonment	
20	**Intermediaries not providing access to information stored on their computer to the relevant authorities**	**Sec 69** imprisonment up to 7 years	
21	**Blocking of websites**	**Sec 69A** imprisonment up to 7 years	
22	**Sending threatening messages by e-mail**		Sec 504 IPC
23	**Sending defamatory messages by email**		Sec 500 IPC
24	**Bogus websites, cyber frauds**	**Sec 66D** 3 years' imprisonment and fine up to Rs 1 lakh	Sec 419 IPC
25	**Email spoofing**	**Sec 66C** 3 years' imprisonment and fine up to Rs 1 lakh	Sec 465 IPC Sec 468 IPC
26	**Making a false document**	**Sec 66D** 3 years' imprisonment and fine up to Rs 1 lakh	Sec 465 IPC
27	**Forgery for purpose of cheating**	**Sec 66D** 3 years' imprisonment and fine up to Rs 1 lakh	Sec 468 IPC
28	**Forgery for purpose of harming reputation**	**Sec 66D** 3 years' imprisonment and fine up to Rs 1 lakh	Sec 469 IPC
29	**Punishment for criminal intimidation**		Sec 506 IPC
30	**Criminal intimidation by anonymous communication**		Sec 507 IPC
31	**Copyright infringement**	**Sec 66** 3 years' imprisonment and fine up to 5 lakh or both	Sec 63, 63B Copyrights Act 1957
32	**Theft of Computer hardware**		Sec 379 IPC
33	**Online sale of drugs**		NDPS Act
34	**Online sale of Arms**		Arms Act