ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳು

[ಕರ್ನಾಟಕ ಸೈಬರ್ ಕೆಫೆ ನಿಯಂತ್ರಣ ಸೂಚನೆ ಮತ್ತು ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯಿದೆ ೨೦೦೦ ಬಗ್ಗೆ ವ್ಯಾಖ್ಯಾನ ಸಹಿತ]

ನಾವಿ

ಪ್ರಕಾಶಕರು

ಉಜ್ವಲ ಕನ್ಸಲ್ಟನ್ಟ್ಸ್ ಪ್ರೈವೇಟ್ ಲಿಮಿಟೆಡ್
ಬೆಂಗಳೂರು

http://www.naavi.org

"Antarjaala Aparaadha"
…a book on Cyber Crimes in Kannada
by

Naavi
[Na.Vijayashankar]

First Edition

Price : Rs 50

Copyright: naavi (2004)

Publisher: Ujvala Consultants Pvt Ltd

Registered office:

37, "Ujvala", 20th Main, B.S.K.Stage I Bangalore 560050.

Administrative Office:

11/10, R.E.Apartments, Unnamalai Ammal Street,
T.Nagar, Chennai, 600017 Ph: 044-28143448
E-Mail: ujvala@eth.net

http://www.naavi.org

ಸೂಚಿಕೆ

.

ಪೀಠಿಕೆ

"ಕಾನೂನು ಮಾಡುವುದು ಸರ್ಕಾರದ ಕೆಲಸ. ಅದನ್ನು ತಿಳಿದು ಅದರಂತೆ ನಡೆದುಕೊಳ್ಳುವುದು ಪ್ರಜೆಗಳ ಜವಾಬ್ದಾರಿ" ಎಂಬ ಅಭಿಪ್ರಾಯ ಕೆಲವರದು. ಆದರೆ ಈ ರೀತಿಯ ಧೋರಣೆಯಿಂದ ಜನರಲ್ಲಿ ಕಾನೂನಿನ ಬಗ್ಗೆ ಹೆದರಿಕೆ ಬರುತ್ತದೆಯೇ ಹೊರತು ಗೌರವ ಬರುವುದಿಲ್ಲ ಮತ್ತು ಜನ ಸಾಮಾನ್ಯರು ಸ್ವಯಿಚ್ಛೆಯಿಂದ ಕಾನೂನನ್ನು ಪಾಲಿಸುವುದಿಲ್ಲ ಎಂಬುದು ನನ್ನ ಅಭಿಮತ.

ಜನರಲ್ಲಿ ಕಾನೂನಿನ ಬಗ್ಗೆ ಅಜ್ಞಾನವಿದ್ದಲ್ಲಿ ಅದರ ಲಾಭ ಜನರ ಅಮಾಯಕತೆಯನ್ನು ದುರುಪಯೋಗ ಮಾಡಿಕೊಳ್ಳುವವರಿಗೆ ಮಾತ್ರ. ಆದ್ದರಿಂದ ಕಾನೂನಿನ ಪರಿಚಯವನ್ನು ಜನ ಸಾಮಾನ್ಯರಿಗೆ ಮಾಡಿಕೊಡಬೇಕಾದುದ್ನು ಸಮಾಜದ ಒಳಿತನ್ನು ಬಯಸುವವರ ಕರ್ತವ್ಯ.

ಮಾಹಿತಿ ತಂತ್ರ ಜ್ಞಾನ ಕಾಯಿದೆ (ಮಾತಂಕಾ–೨೦೦೦) ಭಾರತದಲ್ಲಿ ಕಾನೂನಿನ ರೂಪಕ್ಕೆ ಬಂದು ೪ ವರ್ಷಗಳು ಕಳೆದಿದ್ದರೂ ಅದರ ಬಗ್ಗೆ ಅರಿವು ಇನ್ನೂ ನಮ್ಮ ಜನಗಳಲ್ಲಿ ಮೂಡಿಲ್ಲ. ಜನ ಸಾಮಾನ್ಯರಲ್ಲದೆ, ವಾಣಿಜ್ಯ ವಲಯದಲ್ಲೂ, ಸರ್ಕಾರಿ ಮತ್ತು ಪೋಲೀಸ್ ವಲಯದಲ್ಲೂ ಈ ಕಾನೂನಿನ ಅರಿವು ಇರಬೇಕಾದಷ್ಟು ಇಲ್ಲ. ವಕೀಲರ ಮತ್ತು ನ್ಯಾಯಾಂಗ ವಲಯದಲ್ಲೂ ಈ ಕಾನೂನಿನ ಬಗ್ಗೆ ಹೆಚ್ಚು ತಿಳುವಳಿಕೆ ಮೂಡಿಲ್ಲ ಎಂಬುದು ಸತ್ಯ.

ಇದಕ್ಕೆ ಮುಖ್ಯ ಕಾರಣ ಮಾತಂಕಾ ಅರ್ಥ ಮಾಡಿಕೊಳ್ಳಬೇಕಿದ್ದರೆ ಸ್ವಲ್ಪ ಮಟ್ಟಿಗೆ ತಾಂತ್ರಿಕ ಜ್ಞಾನ ವನ್ನು ರೂಢಿಸಿಕೊಳ್ಳಬೇಕಾದ ಅವಶ್ಯಕತೆಯಿರುವುದು. ನಮ್ಮ ನಾಡಿನ ವಕೀಲರಿಗೆ ಇತ್ತೀಚೆಗಷ್ಟೆ ಕಂಪ್ಯೂಟರ್ ಮತ್ತು ಅದರ ಉಪಯೋಗಗಳ ಬಗ್ಗೆ ಆಸ್ಥೆ ಮೂಡಿದೆ. ಆದ್ದರಿಂದ ಅವರುಗಳು ಈ ಕಾನೂನಿನ ಬಗ್ಗೆ ಇನ್ನೂ ಸರಿಯಾದ ಗಮನ ಹರಿಸಿಲ್ಲ. ತಂತ್ರಜ್ಞರಿಗೆ ಕಾನೂನಿನ ಬಗ್ಗೆ ಹೆಚ್ಚು ಆಸ್ಥೆಯಿಲ್ಲದಿರುವ ಕಾರಣ ಅವರುಗಳೂ ಈ ಕಾನೂನಿನ ಬಗ್ಗೆ ತಿಳಿಸುಕೊಳ್ಳುವ ಪ್ರಯತ್ನ ನಡೆಸಿಲ್ಲ. ಇನ್ನು

ಮೇಲೆಯಾದರೂ ಈ ಎರಡು ವರ್ಗದವರೂ ಈ ಕಾನೂನಿನ ಬಗ್ಗೆ ಹೆಚ್ಚಿನ ಗಮನ ಕೊಡುತ್ತಾರೆಂದು ನಾನು ಆಶಿಸುತ್ತೇನೆ.

ಮಾತಂಕಾ ಮೊದಲ ಬಾರಿ ಪ್ರಕಟವಾಗುವ ಮುಂಚೆಯೇ ೧೯೯೯ ನೇ ಇಸವಿಯಲ್ಲಿ ನಾನು ನನ್ನ ಮೊದಲ ಪುಸ್ತಕ '' ಸೈಬರ್ ಲಾಸ್ ಫ಼ಾರ್ ಎವ್ವೆರಿ ನೆಟಿಜ಼ೆನ್'' ಪ್ರಕಟ ಮಾಡಿದೆ. ನಂತರ ೨೦೦೩ ರಲ್ಲಿ ''ಸೈಬರ್ ಲಾಸ್ ಇನ್ ಇಂಡಿಯಾ..ಐ.ಟಿ.ಎ. ೨೦೦೦ ಎಂಡ್ ಬಿಯಾಂಡ್'' ಎಂಬ ಪುಸ್ತಕವನ್ನು ಇ-ಪುಸ್ತಕದ ರೂಪದಲ್ಲಿ ಬಿಡುಗಡೆ ಮಾಡಿದೆ. ಇತ್ತೀಚೆಗಷ್ಟೆ ''ಸೈಲಾಕಾಂ... ಕಾರ್ಪೊರೇಟ್ ಮಂತ್ರ ಫ಼ಾರ್ ದಿ ಡಿಜಿಟಲ್ ಎರಾ'' ಎಂಬ ಪುಸ್ತಕವನ್ನೂ ಪ್ರಕಟಿಸಿದೆ.

ಈಗ ಜನ ಸಾಮಾನ್ಯರಿಗೆ ಮತ್ತು ಶಾಲಾ ಕಾಲೇಜು ವಿದ್ಯಾರ್ಥಿಗಳಿಗೆ ಉಪಯೋಗವಾಗುವ ಅಂತರ್ಜಾಲ ಅಪರಾಧ ಹಾಗೂ ಸಾಮಾನ್ಯ ಸೈಬರ್ ಕಾನೂನಿನ ಬಗ್ಗೆ ಕನ್ನಡದಲ್ಲಿ ಪ್ರಕಟಮಾಡಬೇಕೆಂಬ ನನ್ನ ಬಯಕೆ ಈ ಪುಸ್ತಕ ರೂಪದಲ್ಲಿ ಹೊರಬಂದಿದೆ.

ಬಹುಶಃ ಭಾರತದಲ್ಲೇ ಮೊದಲ ಬಾರಿಗೆ ಸೈಬರ್ ಕಾನೂನಿನ ಬಗ್ಗೆ ಪ್ರಾದೇಶಿಕ ಭಾಷೆಯಲ್ಲಿ ಪ್ರಕಟವಾದ ಪುಸ್ತಕ ಇದು ಎಂದು ನನ್ನ ಭಾವನೆ.

ಕರ್ನಾಟಕದಲ್ಲಿ ಸೈಬರ್ ಕೆಫ಼ೆ ನಿಯಂತ್ರಣ ಜಾರಿಯಾಗಿರುವ ಮೊದಲ ದಿನಗಳಲ್ಲೇ ಈ ಪುಸ್ತಕ ಪ್ರಕಟವಾಗಿರುವುದು ಸೈಬರ್ ಕೆಫ಼ೆ ಮಾಲೀಕರಿಗೆ ಉಪಯೋಗವಾಗಬಹುದೆಂದು ನನ್ನ ಭಾವನೆ. ಹಾಗೇ ಕಂಪ್ಯೂಟರ್ ಬಗ್ಗೆ ಹಾಗೂ ಅಂತರ್ಜಾಲದ ಬಗ್ಗೆ ವಿದ್ಯೆ ಕಲಿಸುತ್ತಿರುವ ಶಾಲೆಗಳಲ್ಲಿ ಕಂಪ್ಯೂಟರ್ ಅಪರಾಧದ ಬಗ್ಗೆಯೂ ಕೂಡ ತಿಳುವಳಿಕೆ ಕೊಡಬೇಕಾದ ಅಗತ್ಯವನ್ನು ಈ ಪುಸ್ತಕ ಪೂರೈಸಬಹುದು.

http://www.naavi.org

ಇ–ಆಡಳಿತದ ಮುಂಚೂಣಿಯಲ್ಲಿರುವ ನಮ್ಮ ರಾಜ್ಯದ ಅನೇಕ ಸರ್ಕಾರಿ ಕಾರ್ಯಾಲಯಗಳಲ್ಲೂ ಹಳ್ಳಿ ಪ್ರದೇಶಗಳಲ್ಲಿರುವ ರೆವೆನ್ಯೂ ಕಛೇರಿಗಳಲ್ಲೂ ಸೈಬರ್ ಕಾನೂನಿನ ಅರಿವು ಅಗತ್ಯವಾಗಿದೆ. ಈ ಪುಸ್ತಕ ಸ್ವಲ್ಪ ಮಟ್ಟಿಗಾದರೂ ಇಲ್ಲಿಯ ಅಗತ್ಯಗಳನ್ನು ಪೂರೈಸಬಹುದು. ಮುಖ್ಯವಾಗಿ ಸೈಬರ್ ಅಪರಾಧದ ಅರಿವು ರಾಜ್ಯದ ಎಲ್ಲಾ ಪೋಲೀಶ್ ಸ್ಟೇಶನ್ ಗಳಿಗೂ ತಲುಪುವ ಅಗತ್ಯವಿದೆ. ಬಹುಶಃ ಈ ಪುಸ್ತಕದ ಪ್ರಮುಖ ಉಪಯೋಗ ಇಲ್ಲಿ ಆಗಬಹುದು.

ಕನ್ನಡದಲ್ಲಿ ಕಾನೂನಿನ ಬಗ್ಗೆ, ಅದರಲ್ಲೂ ತಾಂತ್ರಿಕ ಕಾನೂನಿನ ಬಗ್ಗೆ ಪುಸ್ತಕ ಬರೆಯುವುದು ಹೊರನಾಡ ಕನ್ನಡಿಗನಾದವನಿಗೆ ಸುಲಭ ಸಾಧ್ಯವಲ್ಲ. ಆದರೂ ಇರುವ ಅಗತ್ಯವನ್ನು ಮನಗೊಂಡು ನನ್ನ ಅರಿವಿನ ಶಬ್ದ ಸಂಪತ್ತಿನೊಳಗೆ ಈ ಪುಸ್ತಕವನ್ನು ಬರೆಯುವುದಕ್ಕೆ ಪ್ರಯತ್ನಿಸಿದ್ದೇನೆ. ಇದರಲ್ಲಿ ಕಾಣಬರುವ ಕನ್ನಡ ಪದಗಳ ಕೊರತೆಯನ್ನು ಮುಂದಿನ ಆವೃತ್ತಿಗಳಲ್ಲಿ ನೀಗುವುದಕ್ಕೆ ಪ್ರಯತ್ನ ಮಾಡುತ್ತೇನೆ. ಈ ವಿಚಾರವನ್ನು ಗಮನಿಸಿ ಓದುಗರು ಈ ಪ್ರಯತ್ನಕ್ಕೆ ಪ್ರೋತ್ಸಾಹ ಕೊಡುತ್ತಾರೆಂದು ನಂಬಿದ್ದೇನೆ.

ನಾ.ವಿಜಯಶಂಕರ [ನಾವಿ]

೧೪.೧೨..೨೦೦೪

ಅಧ್ಯಾಯ ೧ : ಜನಜಾಗೃತಿಯ ಅಗತ್ಯ

ಅಪರಾಧಗಳು ಮಾನವ ಸಮುದಾಯ ಜೀವನದ ಅನಿವಾರ್ಯ ಅಂಗ. ಅಪರಾಧಗಳನ್ನು ತಡೆಯುವುದು, ಅಪರಾಧಿಗಳನ್ನು ಶಿಕ್ಷಿಸುವುದು ಸಮಾಜ ನಿರ್ವಾಹಕರ ಕರ್ತವ್ಯ. ಹಾಗೆಯೇ, ಕಾನೂನುಬದ್ಧ ನಡವಳಿಕೆ ಸುಸಂಸ್ಕೃತ ಪ್ರಜೆಯ ಕರ್ತವ್ಯ ಮತ್ತು ಕಾನೂನು ಶಿಕ್ಷಣ, ಶಿಕ್ಷಕರ ಹಾಗೂ ಪೋಷಕರ ಜವಾಬ್ದಾರಿ. ಈ ಜವಾಬ್ದಾರಿಯನ್ನು ಸಮಾಜದ ಹಿತಚಿಂತಕರು ಅರ್ಥ ಮಾಡಿಕೊಂಡು ನಿಭಾಯಿಸಿದರೆ ಸಮಾಜದಲ್ಲಿ ಅಪರಾಧಗಳ ಸಂಖ್ಯೆ ಕಡಿಮೆಯಾಗಿ ಜನಹಿತಕ್ಕೆ ದಾರಿಯಾಗುತ್ತದೆ.

ಈ ಸಾಮಾಜಿಕ ಜವಾಬ್ದಾರಿಯನ್ನು ನಿರ್ವಹಿಸಬೇಕಿದ್ದರೆ ನಾವು ಮೊದಲು ನಮ್ಮ ಸಾಮಾಜಿಕ ವ್ಯವಸ್ಥೆಯನ್ನು ಅರ್ಥ ಮಾಡಿ ಕೊಂಡು, ಅದರಲ್ಲಿನ ಕಾನೂನಿನ ಚೌಕಟ್ಟನ್ನು ತಿಳಿದುಕೊಂಡು, ಅಪರಾಧಗಳ ರೀತಿಯನ್ನು ಅಧ್ಯಯನ ಮಾಡಿ ನಂತರ ಇತರರಿಗೆ ಮಾರ್ಗದರ್ಶನ ಮಾಡಬೇಕಾದ್ದು ಅವಶ್ಯ.

ಸಮಾಜ ವಿಕಾಸವಾದಂತೆ ಜನ ಜೀವನ ಬದಲಾಗುತ್ತದೆ. ಇದರೊಂದಿಗೆ ಅನೇಕ ಹೊಸ ಹೊಸ ರೀತಿಯ ಅಪರಾಧಗಳು ಹುಟ್ಟಿ ಬರುವುದು ಸಹಜ ಎನ್ನ ಬಹುದು.

ಇಂದು ನಾವಿರುವುದು ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ''ಗಣಕ ಯಂತ್ರ'' ಯುಗ. ನಮ್ಮ ಅನೇಕ ದೈನಂದಿಕ ಕಾರ್ಯಗಳನ್ನು ನಾವು ಮಾಡಲು ಬಳಸುವ ಸಾಧನ ಕಂಪ್ಯೂಟರ್.

ಇಂದು ನಾವು ಕಾಗದ ಬರೆಯಬೇಕಾದರೆ ಲೇಖಣಿ ಇಲ್ಲದೆ ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿ ನೇರವಾಗಿ ಟೈಪ್ ಮಾಡಿ ಪ್ರಿಂಟ್ ತೆಗೆಯುತ್ತೇವೆ. ಹಾಗೆಯೇ, ಕಾಗದ ಪ್ರಿಂಟೂ ಮಾಡದೆ, ಪೋಸ್ಟೂ ಮಾಡದೆ ಇ–ಮೈಲ್ (ಅಂತರ್ಜಾಲ ಪತ್ರ) ಮೂಲಕ ಕಂಪ್ಯೂಟರಿಂದ ಹಾರಿ ಬಿಡುತ್ತೇವೆ. ಮುಂದಿನ ಕ್ಷಣದಲ್ಲಿ ಅದು ನಾವು ಯಾರಿಗೆ ಕಳುಹಿಸಬೇಕೆಂದಿದ್ದೆವೋ ಅವರ ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿ ಅದು ಪ್ರತ್ಯಕ್ಷವಾಗಿರುತ್ತೆ.

ಈ ಕಂಪ್ಯೂಟರ್ ನಿಂದ ಕಂಪ್ಯೂಟರ್ ಗೆ ಬರವಣಿಗೆ ಹಾರುವ ವ್ಯವಸ್ಥೆ ಬಂದದ್ದು ಕಂಪ್ಯೂಟರ್ ಜೋಡಣೆ (ಜಾಲ) ವ್ಯವಸ್ಥೆಯಿಂದ. ಕಂಪ್ಯೂಟರ್ ಜೋಡಣೆ ವ್ಯವಸ್ಥೆ ಹಿಗ್ಗಿದಂತೆ, ದೂರ ದೂರ ಇರುವ ಕಂಪ್ಯೂಟರ್ ಗಳನ್ನೂ ದೂರವಾಣಿ ಅಥವಾ ಕೇಬಲ್ ಗಳ ಮೂಲಕವಾಗಿಯೂ ಹಾಗೂ ಉಪಗ್ರಹ ಮಾಧ್ಯಮ ಮೂಲಕವಾಗಿಯೂ ಸಂಪರ್ಕಿಸಿ, ಜೋಡಿಸುವ ಮೂಲಕ ''ಅಂತರ್ಜಾಲ'' ಎಂಬ ಬೃಹತ್ ಕಂಪ್ಯೂಟರ್ ಜೋಡಣಾ ವ್ಯವಸ್ಥೆಯ ಸೃಷ್ಟಿಯಾಯಿತು.

ಈ ಅಂತರ್ಜಾಲ ವ್ಯವಸ್ಥೆ ಇಂದು ಜಗತ್ತಿನಲ್ಲಿರುವ ಹಲವು ದಶ ಲಕ್ಷ ಕಂಪ್ಯೂಟರ್ ಗಳನ್ನು ಒಂದು ಬೃಹತ್ ಜಾಲದಲ್ಲಿ ಜೋಡಿಸಿದೆ. ಈ ಅಂತರ್ಜಾಲ ವ್ಯವಸ್ಥೆಯ ಮೂಲಕ ನಾವು ಒಂದು ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿರುವ ಯಾವುದೇ ಪದ ಸಮೂಹವನ್ನಾಗಲೀ, ಧ್ವನಿ ಸಂಗ್ರಹವನ್ನಾಗಲೀ ಅಥವಾ ಸ್ಥಿರ ಚಿತ್ರಗಳನ್ನಾಗಲೀ, ಹಾಡು, ಚಲನ ಚಿತ್ರವನ್ನಾಗಲೀ, ಅಥವಾ ಯಾವುದೇ ಸಾಫ್ಟ್ ವೇರ್ (ತಂತ್ರಾಂಶ) ಆಗಲೀ ಅಂತರ್ಜಾಲದಲ್ಲಿ ಸಂಪರ್ಕ ಹೊಂದಿರುವ ಬೇರೆ ಯಾವುದೇ ಕಂಪ್ಯೂಟರ್ ಗೆ ತಕ್ಷಣ ಇ–ಮೈಲ್ ಮೂಲಕ ಕಳುಹಿಸಬಹುದು.

ಅದೇ ರೀತಿ ಯಾವುದೇ ಕಂಪ್ಯೂಟರ್ ಕಡತವನ್ನು ಅಂತರ್ಜಾಲದ ತ್ರಿಶಂಕು ಪಟಲದಲ್ಲಿ ಇಟ್ಟು ಅದನ್ನು ಬೇರೆ ಅಂತರ್ಜಾಲ ಪ್ರವಾಸಿಗಳು ಓದುವ, ಕೇಳುವ ಅಥವಾ ನೋಡುವ ವ್ಯವಸ್ಥೆಯನ್ನು ಮಾಡಬಹುದು. ಈ ಅಂತರ್ಜಾಲ ಕ್ಷೇತ್ರಗಳು ಅಥವಾ ವೆಬ್ ಸೈಟ್ ಗಳು, ಇ–ಮೈಲ್ ನಂತರ ಅಂತರ್ಜಾಲ ವ್ಯವಸ್ಥೆಯ ಬಹು ಮುಖ್ಯ ಅಂಗ.

ಇ–ಮೈಲ್ ಮತ್ತು ವೆಬ್ ಸೈಟ್ ಗಳಲ್ಲದೆ, ಅಂತರ್ಜಾಲದಲ್ಲಿ ಒಬ್ಬರೊಡನೆ ಇನ್ನೊಬ್ಬರು ಒಂದೇ ಸಮಯದಲ್ಲಿ ದೂರವಾಣಿಯಲ್ಲಿ ಮಾತನಾಡುವಂತೆ ಬರವಣಿಗೆಯಲ್ಲಿ ವ್ಯವಹರಿಸಬಹುದು. ಇದಕ್ಕೆ ''ಚ್ಯಾಟ್ ಮಾಡುವುದು'' ಅಥವಾ

''ಹರಟುವುದು'' ಎಂದು ಕರೆಯುತ್ತಾರೆ. ಈ ಹರಟೆ ವ್ಯವಹಾರ ಕೂಡ ಅಂತರ್ಜಾಲದ ಮುಖ್ಯ ಅಂಗಗಳಲ್ಲೊಂದು.

ಅಂತರ್ಜಾಲದ ನಾಲ್ಕನೇ ಮುಖ್ಯ ಅಂಗವೇನೆಂದರೆ, ''ಸೂಚನಾ ಫಲಕಗಳು'' ಅಥವಾ ಮೆಸೇಜ್ ಬೋರ್ಡ್ ಗಳು. ಈ ಅಂತರ್ಜಾಲ ಸೂಚನಾ ಫಲಕಗಳಲ್ಲಿ ಒಬ್ಬರು ಏನಾದರೂ ಸಮಾಚಾರವನ್ನು ಬರೆದರೆ, ಮತ್ತೊಬ್ಬರು ನಂತರ ಬಂದು ಅದನ್ನು ಓದಿಕೊಳ್ಳಬಹುದು.

ಈ ಮೇಲ್ಕಂಡ ಇ–ಮೈಲ್, ವೆಬ್ ಸೈಟ್, ಚ್ಯಾಟ್, ಮತ್ತು ಮೆಸೇಜ್ ಬೋರ್ಡ್ (ಅಥವಾ ಅಂತರ್ಜಾಲ ಪತ್ರ, ಅಂತರ್ಜಾಲ ಕ್ಷೇತ್ರ, ಅಂತರ್ಜಾಲ ಹರಟೆ, ಹಾಗೂ ಅಂತರ್ಜಾಲ ಸೂಚನಾ ಫಲಕ) ಇಂದಿನ ಪೀಳಿಗೆಯ ಅತಿ ಮುಖ್ಯ ಸಂಪರ್ಕ ಸಾಧನ ಗಳಾಗಿವೆ ಎನ್ನಬಹುದು. ಕಂಪ್ಯೂಟರ್ ಬರವಣಿಗೆ, ಕಂಪ್ಯೂಟರ್ ಮಾತು, ಕಂಪ್ಯೂಟರ್ ದೃಶ್ಯ ತುಂಬಿರುವ ಈ ಅಂತರ್ಜಾಲ ಯುಗ ನಮ್ಮ ಜೀವನ ಹಾಗೂ ಸಂಸ್ಕೃತಿಯಲ್ಲಿ ಊಹಿಸಲಾರದ ಬದಲಾವಣೆಗಳನ್ನು ತಂದಿದೆ.

ಇಂದು ವೈಯುಕ್ತಿಕ ಸಂಭಾಷಣೆಗಲ್ಲದೆ ಅಂತರ್ಜಾಲ ಒಂದು ಜಾಗತಿಕ ವಾಣಿಜ್ಯ ವ್ಯವಹಾರ ಕೇಂದ್ರವಾಗಿ ಕೂಡಾ ಬೆಳೆದು ಬಂದಿದೆ. ಅಂತರ್ಜಾಲದಲ್ಲಿ ಇಂದು ಹಣ ಕ್ಕೆಬದಲಾಯಿಸುವ ವ್ಯವಸ್ಥೆ ಇದೆ. ಇದರಿಂದಾಗಿ ಅನೇಕಾನೇಕ ಇ–ಕಾಮರ್ಸ್ (ಅಂತರ್ಜಾಲ ವಾಣಿಜ್ಯ ಕೇಂದ್ರ) ವೆಬ್ ಸೈಟ್ ಗಳು ಅಂತರ್ಜಾಲ ಮಳಿಗೆಗಳನ್ನು ತೆಗೆದು ಹಲವಾರು ಪದಾರ್ಥಗಳನ್ನೂ, ಸೇವೆಗಳನ್ನೂ ಮಾರಾಟ ಮಾಡುತ್ತಿವೆ. ಬ್ಯಾಂಕು ಗಳು ಅಂತರ್ಜಾಲದ ಮೂಲಕ ಗ್ರಾಹಕರೊಡನೆ ವ್ಯವಹರಿಸುತ್ತಿವೆ. ಶೇರುಪೇಟೆಗಳು ಶೇರುಗಳನ್ನು ಕೊಳ್ಳುವ ಹಾಗೂ ಮಾರಾಟಮಾಡುವ ಅಂತರ್ಜಾಲ ಶೇರು ಮಾರುಕಟ್ಟೆಗಳನ್ನು ನಡೆಸುತ್ತಿವೆ. ಅನೇಕ ವೆಬ್ ಸೈಟ್ ಗಳು ಅಂತರ್ಜಾಲ ಶಾಲೆಗಳನ್ನೂ, ಮನರಂಜನಾ ಕೇಂದ್ರಗಳನ್ನೂ, ದೇವಸ್ಥಾನ/ಪೂಜಾ ಕೇಂದ್ರಗಳನ್ನೂ ನಡೆಸುತ್ತಿವೆ.

ಇತ್ತೀಚಿನ ವರ್ಷಗಳಲ್ಲಿ ಸರ್ಕಾರಗಳು ಸಹ ಜನರೊಡನೆಯ ತಮ್ಮ ಅನೇಕ ವ್ಯವಹಾರಗಳಿಗೆ ಅಂತರ್ಜಾಲವನ್ನು ಬಳಸುತ್ತಿದೆ. ಕರ್ನಾಟಕ ಸರ್ಕಾರದಲ್ಲಿ "ಭೂಮಿ" ಅಂತಹ ಸೇವಾ ವ್ಯವಸ್ಥೆಯ ಮೂಲಕ ಸಾಮಾನ್ಯ ರೈತರುಗಳ ವ್ಯವಸಾಯ ವಿವರಗಳೂ, ಹಕ್ಕು ಪತ್ರಗಳೂ ಇಂದು ಅಂತರ್ಜಾಲ ವ್ಯವಸ್ಥೆಗೆ ಬದಲಾಯಿಸಲ್ಪಟ್ಟಿವೆ. ಹಾಗೆಯೇ, ವಿದ್ಯುಚ್ಛಕ್ತಿ, ನೀರು, ಕಂದಾಯ, ದೂರವಾಣಿ ಮುಂತಾದ ಸೇವೆಗಳಿಗೆ ಅಂತರ್ಜಾಲದ ಮೂಲಕ ಹಣ ಕಟ್ಟುವ ವ್ಯವಸ್ಥೆ ಬೆಳೆದು ಬರುತ್ತಿದೆ. ಇನ್ನು ಕೆಲವು ವರ್ಷಗಳಲ್ಲಿ ಇ–ಆಡಳಿತ ಅಥವಾ ಇ–ಆಳ್ವಿಕೆ ಇಂದಿನ ಸರ್ಕಾರದ ಮುಖ್ಯ ವ್ಯವಸ್ಥೆಯಾಗುವುದು ಸಂದೇಹರಹಿತ.

ಈ ರೀತಿ ನಮ್ಮ ಸುತ್ತಲಿನ ಸಮಾಜ ಅಂತರ್ಜಾಲ ಕ್ಷೇತ್ರವಾಗಿ ಬದಲಾವಣೆಯಾದಾಗ, ನಾವೆಲ್ಲರೂ, ಈ ಸಾಮಾಜಿಕ ಆಂದೋಲನದಿಂದ ಹಲವಾರು ರೀತಿ ಮಾರ್ಪಾಡಿನ ಸುಳಿಯಲ್ಲಿ ಸಿಕ್ಕಿಬೀಳುತ್ತೇವೆ. ಇದರಲ್ಲಿ ಕಂಪ್ಯೂಟರ್ ಉಪಯೋಗಿಸುವವರಲ್ಲದೆ, ಉಪಯೋಗಿಸದೇ ಇರುವವರೂ ಅನೇಕ ರೀತಿಯಲ್ಲಿ ಪ್ರಭಾವಿತರಾಗುತ್ತಾರೆ.

ಒಂದು ವಿಧದಲ್ಲಿ ಈ ಪ್ರಭಾವ ನಮ್ಮ ಜೀವನವನ್ನು ಉತ್ತಮಪಡಿಸುವ ಹಾದಿಯಲ್ಲಿರುತ್ತದೆ ಎಂಬುದು ನಿರ್ವಿವಾದ. ಅದೇ ಸಮಯದಲ್ಲಿ, ಅಂತರ್ಜಾಲ ಸಮಾಜದಲ್ಲಿನ ಹಲವು ದುಷ್ಟ ಶಕ್ತಿಗಳಿಂದ ಅಪರಾಧಗಳೂ ಬೆಳೆದುಬರುವುದು ಸಹಜ. ಈ ಅಪರಾಧಗಳಿಂದ ಅನೇಕ ಮುಗ್ಧ ಜನರಿಗೆ ಅನಾನುಕೂಲಗಳೂ, ನಷ್ಟಗಳೂ ಒದಗುವುದು ಕಟ್ಟಿಟ್ಟ ಬುತ್ತಿ.

ಅಂತರ್ಜಾಲದ ಉಪಯೋಗಗಳನ್ನು ತಿಳಿದಿರುವ ಜನರು ಈ ಅಂತರ್ಜಾಲ ಕ್ರಾಂತಿಯಿಂದ ಒಂದು ಜಾಗತಿಕ ಬದಲಾವಣೆಯನ್ನು ಎದುರುನೋಡುತ್ತಿರುವಂತೆ, ಈ

ಕ್ರಾಂತಿಯಲ್ಲಿ ಅಮಾಯಕರ ಶೋಷಣೆಯಾಗದಂತೆ ನೋಡಿಕೊಳ್ಳುವ ಜವಾಬ್ದಾರಿಯನ್ನು ಹೊಂದಿರುವರೆಂದು ನನ್ನ ಅಭಿಮತ.

ಅಂತೆಯೇ, ಮಕ್ಕಳಿಗೆ ಕಂಪ್ಯೂಟರ್ ಕೊಡಿಸಿ, ಅಂತರ್ಜಾಲ ಸಂಪರ್ಕವನ್ನು ಕೊಡಿಸುವ ತಾಯ್ತಂದೆಯರೂ, ಶಾಲಾ ಕಾಲೇಜುಗಳಲ್ಲಿ ಅಂತರ್ಜಾಲದ ಬಗ್ಗೆ ಮಾಹಿತಿ ಕೊಟ್ಟು ಕಂಪ್ಯೂಟರ್ ಬಳಕೆಯನ್ನು ಕಲಿಸಿಕೊಡುವ ಶಿಕ್ಷಕರೂ, ದೇಶದ ಜನತೆಗೆ ಇ–ಆಡಳಿತದ ಸವಿಯನ್ನುಣಿಸಲು ಸಿದ್ಧವಾಗಿರುವ ಸರ್ಕಾರಿ ನಿರ್ವಾಹಕರೂ ಮತ್ತು ಜನ ನಾಯಕರೂ, ಕಂಪ್ಯೂಟರ್ ಬಳಕೆಯಿಂದ ಲಾಭಗಳಿಸುತ್ತಿರುವ ಎಲ್ಲಾ ಉದ್ಯಮಿಗಳೂ ಅಂತರ್ಜಾಲದ ಅಪರಾಧಗಳಿಂದ ಜನ ಸಾಮಾನ್ಯರಿಗೆ ತೊಂದರೆಯಾಗದಂತೆ ತಡೆಯುವ ಜವಾಬ್ದಾರಿಯನ್ನು ಹೊಂದಿದ್ದಾರೆ.

ಜನ ಸಾಮಾನ್ಯರಲ್ಲಿ ಅಂತರ್ಜಾಲ ಅಪರಾಧ (ಸೈಬರ್ ಕ್ರೈಮ್) ಗಳ ಬಗ್ಗೆ ಜಾಗ್ರತೆಮೂಡಿಸಿ ಅವರುಗಳು ಎಚ್ಚರವಾಗಿರುವಂತೆ ಮಾಡುವುದೇ ಈ ಪುಸ್ತಕದ ಮೂಲ ಉದ್ದೇಶ. ಹಾಗೇ ಭಾರತದಲ್ಲಿರುವ ಸೈಬರ್ ಕಾನೂನಿನ ಬಗ್ಗೆ ಸಾಮಾನ್ಯ ಜ್ಞಾನ ಒದಗಿಸುವುದೂ ಈ ಪುಸ್ತಕದ ಉದ್ದೇಶವಾಗಿದೆ.

ಅಧ್ಯಾಯ ೨ ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳು

ಅಂತರ್ಜಾಲದಲ್ಲಿ ಅನೇಕ ರೀತಿಯ ಅಪರಾಧಗಳನ್ನು ನಾವು ಕಾಣಬಹುದು. ಇದರಲ್ಲಿ ಕೆಲವು ಅಪರಾಧಗಳು ಕಂಪ್ಯೂಟರ್ ಕ್ಷೇತ್ರಕ್ಕೇ ಸೇರಿದವುಗಳು. ಇನ್ನು ಕೆಲವು ಅಪರಾಧಗಳು ಭಾರತೀಯ ಅಪರಾಧ ಸಂಹಿತೆಯಲ್ಲಿ ಈಗಾಗಲೇ ಉಲ್ಲೇಖಿಸರಾಗಿರುವ ಅಪರಾಧಗಳು. ಈ ಸಾಮಾನ್ಯ ಅಪರಾಧಗಳು ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ಅಂತರ್ಜಾಲವನ್ನು ಉಪಯೋಗಿಸಿ ಮಾಡಲ್ಪಟ್ಟಿದ್ದರೆ ಅವುಗಳನ್ನು ಕೂಡ ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳ ಪಟ್ಟಿಯಲ್ಲಿ ಸೇರಿಸಬೇಕಾಗುತ್ತದೆ. ಏಕೆಂದರೆ ಈ ಅಪರಾಧಗಳನ್ನು ನ್ಯಾಯಾಲಯದಲ್ಲಿ ಪ್ರಸ್ತುತಪಡಿಸಿ ಕ್ರಮ ಜರುಗಿಸಬೇಕಾದರೆ ಸೈಬರ್ ಸಾಕ್ಷಿಯನ್ನು ನ್ಯಾಯಾಲಯಕ್ಕೆ ಒಪ್ಪಿಗೆಯಾಗುವಂತೆ ಹೊಂದಿಸಿ ಪ್ರಸ್ತುತ ಪಡಿಸಬೇಕಾಗುತ್ತದೆ. ಈ ದೃಷ್ಟಿಯಿಂದ ಅಂತರ್ಜಾಲದ ಮೂಲಕ ನಡೆಯುವ ಸಾಮಾನ್ಯ ಅಪರಾಧಗಳ ಬಗ್ಗೆ ಕೂಡಾ ಇಲ್ಲಿ ಸಂಕ್ಷಿಪ್ತವಾಗಿ ಪ್ರಸ್ತಾವಿಸಲಾಗಿದೆ.

೧. ಸೈಬರ್ ಮೋಸ:

ಮೋಸ ವೆಂದರೆ ಒಬ್ಬರನ್ನು ತಪ್ಪು ಮಾಹಿತಿಯಿಂದ ವಂಚಿಸಿ ಹಣದ ಅಥವಾ ಬೇರಾವುದೇ ರೀತಿಯ ಲಾಭವನ್ನು ಪಡೆದುಕೊಳ್ಳುವುದು ಎನ್ನಬಹುದು.

ಅಂತರ್ಜಾಲ ಇಂದು ಹೊಂದಿರುವ ಲಕ್ಷಾಂತರ ವೆಬ್ ಸೈಟ್ ಗಳಲ್ಲಿ ಅನೇಕ ರೀತಿಯ ಮಾಹಿತಿ ಇರುವುದರಿಂದ ಜನ ಸಾಮಾನ್ಯರು ಅಗಾಗ್ಗೆ ಈ ವೆಬ್ ಸೈಟ್ ಗಳಿಗೆ ಹೋಗಿ ಅಲ್ಲಿರುವ ಮಾಹಿತಿಯನ್ನು ಪಡೆಯುವುದು ಸಹಜ. ಅದೇ ರೀತಿ ಯಾವುದಾದರೂ ಇ–ಮೈಲ್ ಬಂದರೆ ಅದರಲ್ಲಿರುವ ಮಾಹಿತಿ ನಂಬಲರ್ಹವೆಂದುಕೊಳ್ಳುವುದೂ ಸಹಜ. ಅಂತರ್ಜಾಲ ಮೋಸ ಪ್ರಕರಣಗಳಲ್ಲಿ ಮುಖ್ಯವಾಗಿ ವಂಚಕರು ಉಪಯೋಗಿಸುವುದು ''ಸುಳ್ಳು ವೆಬ್ ಸೈಟ್''ಗಳು.

ಉದಾಹರಣೆಗೆ ಕೆಲವು ವರ್ಷಗಳ ಹಿಂದೆ ನಮ್ಮಲ್ಲಿ ಒಂದು ವಂಚನೆ ಪ್ರಕರಣ ಬೆಳಕಿಗೆ ಬಂದಿತು. ಇದರಲ್ಲಿ ಆಂಧ್ರದ ಒಬ್ಬ ವ್ಯಾಪಾರಿ ಒಂದು ಅಂತರ ರಾಷ್ಟ್ರೀಯ ಲಾಟರಿಯಲ್ಲಿ ಹಲವು ಕೋಟಿ ರೂಪಾಯಿ ಗೆದ್ದಿರುವ ಆಧಾರದ ಮೇಲೆ ಇಲ್ಲಿಯ ಬ್ಯಾಂಕುಗಳಲ್ಲಿ ಸಾಲ ತೆಗೆದುಕೊಂಡು ವಂಚನೆ ಮಾಡಿರುವುದಾಗಿ ಆಪಾದಿಸಲಾಗಿತ್ತು. ಈ ಪ್ರಸಂಗದಲ್ಲಿ ತಾನು ಲಾಟರಿಯಲ್ಲಿ ಬಹುಮಾನ ಪಡೆದಿರುವುದಕ್ಕೆ ಒಂದು ವೆಬ್ ಸೈಟ್ ನಲ್ಲಿರುವ ಮಾಹಿತಿಯನ್ನು ಆಧಾರವಾಗಿ ಆಪಾದಿತ ತೋರಿಸಿರುವುದಾಗಿಯೂ ಮತ್ತು ಅದು ಸುಳ್ಳಾಗಿತ್ತೆಂದೂ ತಿಳಿಸಲಾಗಿತ್ತು.

ಮುಖ ನೋಟಕ್ಕೆ ಇದು ತಿಳಿಯಾದ ಮೋಸ ಪ್ರಸಂಗದಂತೆ ಕಾಣಬಹುದು. ಆದರೆ ಇದರ ಹಿಂದೆ ಒಂದು ದೊಡ್ಡ ಅಂತರ್ಜಾಲ ವಂಚನೆಯ ಯೋಜನೆ ಇದ್ದು ಇದರಲ್ಲಿ ಆಂಧ್ರದ ಆಪಾದಿತ ಮಹಾಶಯ ಬಹುಶಃ ಒಬ್ಬ ಅಮಾಯಕ ಬಲಿಪಶು (ವಿಕ್ಟಿಮ್) ಆಗಿರಬಹುದು. ಈ ಲಾಟರಿ ಬಹುಮಾನ ವಂಚನೆ ಈಗಲೂ ನಾವು ಕಾಣಬರುವ ಮೋಸ ಪ್ರಸಂಗಗಳಲ್ಲೊಂದು.

ಈ ಮೋಸದ ವೈಖರಿ ಹೀಗಿರುತ್ತದೆ.

ಮೊದಲು ಸಾಮಾನ್ಯವಾಗಿ ಒಬ್ಬರಿಗೆ ಇ–ಮೈಲ್ ಮೂಲಕ ಅವರು ದೊಡ್ಡ (ಸುಮಾರು ೫ ಕೋಟಿ ರೂಪಾಯಿ ಇರಬಹುದು) ಲಾಟರಿ ಬಹುಮಾನ ಪಡೆದಿರುವುದಾಗಿಯೂ ಅದನ್ನು ಪಡೆದುಕೊಳ್ಳಲು ತಮ್ಮ ಇ–ಮೈಲ್ ವಿಳಾಸವನ್ನು ಧೃಢೀಕರಿಸಿದರೆ ಸಾಕೆಂದು ಒಂದು ಇ–ಮೈಲ್ ಬರುತ್ತದೆ. ಇದಕ್ಕೆ ಬದಲು ನೀಡಿದರೆ, ನಂತರ ಮುಂದಿನ ಇ–ಮೈಲ್ ಗಳಲ್ಲಿ, ಇನ್ನೇನು ನಿಮಗೆ ಹಣ ಕಳುಹಿಸಿಬಿಡುತ್ತೇವೆ, ದಯವಿಟ್ಟು ನಮ್ಮ ಕಮಿಶನ್ ನೂರು ಡಾಲರ್ ಕಳುಹಿಸಿ ಎಂದು ನಯವಾದ ಕಾಗದ ಬರುತ್ತದೆ. ಇದನ್ನು ನಂಬಿ ಹಣ ಕಳುಹಿಸಿದರೆ ಅದು ಗೋವಿಂದ.

ಈ ಮೋಸಕ್ಕೆ ಪುಷ್ಟಿ ಕೊಡಲು ಮೋಸಗಾರರ ಕಡೆಯಿಂದ ಫೋನ್ ನಲ್ಲಿ ಮಾತನಾಡಿ ನಾವು ಲಾಟರಿ ಸಂಸ್ಥೆಯ ಆಡಿಟರ್ ಅಥವಾ ಬ್ಯಾಂಕ್ ನವರೆಂದೂ ನಂಬಿಸುವುದೂ ಉಂಟು. ಈ ರೀತಿಯ ಮೋಸದ ಲಾಟರಿ ಬಲೆಯಲ್ಲಿ ಲಕ್ಷಾಂತರ ರೂಪಾಯಿ ಕಳೆದುಕೊಂಡವರ ಉದಾಹರಣೆ ಇದೆ.

ಆಂಧ್ರ ಪ್ರಕರಣ ಈರೀತಿಯ ಪ್ರಕರಣವೋ ಅಥವಾ ನಿಜವಾಗಿಯೂ ಆಪಾದಿತ ತಾನೇ ಸುಳ್ಳು ವೆಬ್ ಸೈಟ್ ಮಾಡಿ ಮೋಸ ಮಾಡುವುದಕ್ಕೆ ಪ್ರಯತ್ನ ಪಟ್ಟನೋ ನಮಗೆ ತಿಳಿದಿಲ್ಲ. ಆದರೆ ಈ ಲಾಟರಿ ಬಹುಮಾನದ ಇ-ಮೈಲ್ ಬಗ್ಗೆ ಯಾವ ಕಾಳಜಿಯನ್ನೂ ತೋರದಿರುವುದು ಕ್ಷೇಮ.

ನೈಜೀರಿಯನ್ ವಂಚನೆ ಎಂಬ ಮತ್ತೊಂದು ವಂಚನೆ ಜಾಲ ದಲ್ಲಿ ಇನ್ನೊಂದು ಬಗೆಯ ಇ-ಮೈಲ್ ಬರುತ್ತದೆ. ಇದರಲ್ಲಿ ನಾನು ನೈಜೀರಿಯ ಮಾಜಿ ಅಧ್ಯಕ್ಷರ ವಿಧವೆಯೆಂದೂ, ತನ್ನ ಬಳಿ ಸುಮಾರು ೧೦೦ ಕೋಟಿ ರೂಪಾಯಿ ಬ್ಯಾಂಕ್ ಖಾತೆಯಲ್ಲಿರುವುದಾಗಿಯೂ, ಅದನ್ನು ದೇಶದಿಂದ ಹೊರಗೆ ಸಾಗಿಸಲು ಸಹಾಯ ಮಾಡಿದರೆ ನಿಮಗೆ ೫% ಕಮಿಶನ್ ನೀಡುವುದಾಗಿಯೂ ತಿಳಿಸಲಾಗುತ್ತದೆ. ಇದಕ್ಕೆ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ವಿವರ ಕೊಟ್ಟರೆ ಸಾಕು ಆದಕ್ಕೆ ಹಣ ವರ್ಗಾವಣೆ ಮಾಡುವುದಾಗಿಯೂ ತಿಳಿಸಿರುತ್ತೆ. ಕೆಲವು ಬಾರಿ ಇದೇ ರೀತಿಯ ಇ-ಮೈಲ್, ಸದ್ದಾಮ್ ಹುಸೈನ್ ನ ನೆಂಟರಂತೆಯೂ, ನೇಪಾಳದ ಮಾಜಿ ರಾಜ ಬಿರೇಂದ್ರ ವಿಕ್ರಂ ನ ನೆಂಟರಂತೆಯೂ ಅಥವಾ ಒಂದು ಪೆಟ್ರೋಲಿಯಂ ಕಂಪನಿಯ ಮಾಲೀಕನ ಹೆಸರಿನಲ್ಲೂ ಬಂದದ್ದಿದೆ. ಈ ಎಲ್ಲಾ ವಂಚನೆಗಳ ಉದ್ದೇಶ ನಮ್ಮಿಂದ ಕಮಿಶನ್ ರೂಪದಲ್ಲಿ ಸುಮಾರು ೧೦೦೦ ದಿಂದ ೫೦೦೦ ಡಾಲರ್ ಹೊಡೆಯುವುದು. ಕೆಲವು ಪ್ರಸಂಗಗಳಲ್ಲಿ ಜನಗಳನ್ನು ನೈಜೀರಿಯ ಅಥವಾ ಲಂಡನ್ ಗೆ ಹೆಚ್ಚಿನ ಮಾತುಕತೆಗೆ ಆಹ್ವಾನಿಸಿ ಅಪಹರಣ ಮಾಡಿ ಕೊಲೆ ಮಾಡಿರುವ ಸಾಧ್ಯತೆಗಳೂ ಇವೆ ಎಂದು ಎಫ್ಬಿಐ ತಿಳಿಸಿದೆ.

ಇದೇ ರೀತಿ ಸಂಭಾಷಣೆ ಆರಂಭಿಸಿ ನಂಬಿದ ಜನರನ್ನು ಹವಾಲ (ವಿದೇಶಿ ಹಣ ಬದಲಾವಣೆ) ವ್ಯವಹಾರಕ್ಕೆ ಬಳಸಿಕೊಳ್ಳುವ ಪ್ರಯತ್ನಗಳೂ ಭಾರತದಲ್ಲಿಯೇ ಬೆಳಕಿಗೆ ಬಂದಿದೆ.

ಇತ್ತೀಚಿನ ಪ್ರಸಂಗವೊಂದರಲ್ಲಿ ಬಿ.ಬಿ.ಸಿ. ವೆಬ್ ಸೈಟ್ ನಲ್ಲಿನ ಒಂದು ಲೇಖನದಲ್ಲಿ ಇರಾಕ್ ನಲ್ಲಿನ ವ್ಯಕ್ತಿಯೊಬ್ಬನ ವಿಚಾರ ಪ್ರಕಟವಾಗಿತ್ತು. ಇದರಲ್ಲಿ ಈ ವ್ಯಕ್ತಿಗೆ ಹಿಂದಿನ ಇರಾಕ್ ಸರ್ಕಾರದಿಂದ ಅನೇಕ ತೊಂದರೆಯಾಗಿತ್ತೆಂದೂ, ಅವನನ್ನು ಅನೇಕ ರೀತಿಯ ಹಿಂಸೆಗೆ ಗುರಿಪಡಿಸಲಾಗಿತ್ತೆಂದೂ ಬರೆಯಲಾಗಿತ್ತು. ಲೇಖನದ ಉದ್ದೇಶಕ್ಕೋಸ್ಕರ ಆ ವ್ಯಕ್ತಿಯ ನೈಜ ವಾದ ಹೆಸರನ್ನು ಮರೆಸಿ ''ಮಹಮದ್'' ಎಂದು ಉಪಯೋಗಿಸಲಾಗಿತ್ತು. ಈ ಹೆಸರು ಬದಲಾವಣೆ ಲೇಖನದ ಪುಟದಲ್ಲಿ ಒಂದು ಮೂಲೆಯಲ್ಲಿ ಪ್ರಕಟವಾಗಿತ್ತು. ಚಾಣಾಕ್ಷ ನೈಜೀರಿಯನ್ ಮೋಸಗಾರನೊಬ್ಬ ತಾನು ಕಳುಹಿಸಿದ ಮೋಸದ ಇ–ಮೈಲ್ ನಲ್ಲಿ ತನ್ನ ಹೆಸರು ಮಹಮದ್ ಎಂದೂ, ತನಗೆ ಇರಾಕ್ ಸರ್ಕಾರದಿಂದ ಅನ್ಯಾಯವಾಗಿರುವುದೆಂದೂ ತಿಳಿಸಿ, ಈ ಬಗ್ಗೆ ಬಿ.ಬಿ.ಸಿ. ವೆಬ್ ಸೈಟ್‌ನಲ್ಲಿ ಪ್ರಕಟವಾಗಿರುವುದೆಂದು ತಿಳಿಸಿ ಆ ಲೇಖನವನ್ನು ಉಲ್ಲೇಖಿಸಿದ್ದಾನೆ. ಬಿ.ಬಿ.ಸಿ. ವೆಬ್ ಸೈಟನ್ನು ನಂಬಿ ಈ ವ್ಯಕ್ತಿಯ ಇ–ಮೈಲ್ ನಂತೆ ನಡೆದರೆ ನಾವು ಮೋಸದ ಬಲೆಯಲ್ಲಿ ಸಿಕ್ಕಿಬೀಳುವುದು ಖಂಡಿತ.

ಬೇರೊಂದು ಬಗೆಯ ಮೋಸದಲ್ಲಿ ಕಿಡಿಗೇಡಿಗಳು ಏನು ಮಾಡುತ್ತಾರೆಂದರೆ, ನಮಗೆಲ್ಲಾ ತಿಳಿದಿರುವ ಸಿಟಿ ಬ್ಯಾಂಕ್ ಅಥವಾ ಹಾಂಕಾಂಗ್ ಬ್ಯಾಂಕ್ ತರಹದ ಬ್ಯಾಂಕ್ ಹೆಸರಿನಲ್ಲಿ ಒಂದು ಸುಳ್ಳು ವೆಬ್ ಸೈಟ್ ಸೃಷ್ಟಿಮಾಡಿ ''ನೀವು ಬ್ಯಾಂಕ್ ಗ್ರಾಹಕರಾಗಿದ್ದರೆ ಒಡನೆಯೇ ಈ ವೆಬ್ ಸೈಟ್ ಗೆ ಹೋಗಿ ಖಾತೆ ಸರಿಯಾಗಿದೆಯೇ ಎಂದು ಪರೀಕ್ಷಿಸಿ'' ಎಂದು ಇ–ಮೈಲ್ ಮೂಲಕ ಎಲ್ಲರಿಗೂ ಸುದ್ದಿ ಕೊಡುತ್ತಾರೆ. ಹಾಗೆ ಯಾರಾದರೂ ಈ ಸುಳ್ಳು ವೆಬ್ ಸೈಟ್ ಗೆ ಹೋಗಿ ತಮ್ಮ ಪಾಸ್ ವರ್ಡ್ ಉಪಯೋಗಿಸಿ (ಖಾತೆಯನ್ನು ಅಂತರ್ಜಾಲದ ಮೂಲಕ ನಿರ್ವಹಿಸುವುದಕ್ಕೆ ಬೇಕಾದ ಗುಟ್ಟಾಗಿಡಬೇಕಾದ ಪ್ರವೇಶ ಪದ) ಪರೀಕ್ಷಿಸಿದರೆ, ಒಡನೆಯೇ ಆ ಪಾಸ್ ವರ್ಡ್

ಕದ್ದು ನಂತರ ತಾವು ನಿಜವಾದ ಬ್ಯಾಂಕ್ ವೆಬ್ ಸೈಟ್ ಗೆ ಹೋಗಿ ಹಣ ದೋಚಿಕೊಂಡು ಪರಾರಿಯಾಗುತ್ತಾರೆ.

ಈ ಪ್ರಕರಣಗಳಲ್ಲಿ ನಾವು ಮುಖ್ಯವಾಗಿ ನೆನಪಿನಲ್ಲಿಡಬೇಕಾದ ಅಂಶ ವೇನೆಂದರೆ, ನಮಗೆ ಬರುವ ಇ–ಮೈಲ್ ಗಳಲ್ಲಿರುವ ವಿಷಯಗಳನ್ನೆಲ್ಲಾ ನಂಬಿ ಮೋಸ ಹೋಗ ಬಾರದು. ಹಾಗೇ ವೆಬ್ ಸೈಟ್ ಗಳಲ್ಲಿ ಸುಳ್ಳು ವೆಬ್ ಸೈಟ್ ಗಳೂ ಇರುತ್ತವೆಂದು ನಾವು ತಿಳಿದಿರಬೇಕು.

ಹಾಗೆಯೇ ಇಂತಹ ಪ್ರಕರಣಗಳು ನಮ್ಮ ಗಮನಕ್ಕೆ ಬಂದರೆ ಆದನ್ನು ಪೋಲೀಸರ ಗಮನಕ್ಕೆ ತರಲು ಪ್ರಯತ್ನ ಪಡಬಹುದು.

ಭಾರತದಲ್ಲಿರುವ ಸೈಬರ್ ಕಾನೂನಿನ ಪ್ರಕಾರ ಸೈಬರ್ ಮೋಸದಿಂದ ವಂಚಿತರಾದವರು ವಿಶೇಷ ಕಾನೂನು ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ''ಅಡ್ಜುಡಿಕೇಟರ್'' (ಸೈಬರ್ ನಿರ್ಣಯಕಾರ) ಮೂಲಕ ಅಪರಾಧಿಗಳಿಂದ ಒಂದು ಕೋಟಿ ರೂಪಾಯಿವರೆವಿಗೆ ನಷ್ಟ ಪರಿಹಾರ ಕೇಳಬಹುದು. (ಇದು ಎಲ್ಲಾ ಮೋಸಗಳಿಗೂ ಅನ್ವಯವಾಗದೇ ಇರಬಹುದು. ಆದರೆ ಅಂತರ್ಜಾಲದಲ್ಲಿನ ಮಾಹಿತಿಯನ್ನು ಬದಲಾಯಿಸಿ ಮಾಡುವ ಅನೇಕ ಮೋಸದ ಪ್ರಸಂಗಗಳಿಗೆ ಇದು ಅನ್ವಯವಾಗುತ್ತದೆ.)

ಅಂತೆಯೇ, ನಾವು ನ್ಯಾಯವಾಗಿ ಅಂತರ್ಜಾಲದ ಮೂಲಕ ಮಾಡುವ ವ್ಯವಹಾರವನ್ನು ಬೇರೆಯವರು ನಂಬಬೇಕಿದ್ದರೆ ಸೈಬರ್ ಕಾನೂನಿನಲ್ಲಿ ತಿಳಿಸಿರುವ ಡಿಜಿಟಲ್ ಸಿಗ್ನೇಚರ್ ಅಥವಾ ''ಡಿಜಿಟಲ್ ಸಹಿ'' ಯನ್ನು ನಮ್ಮ ಇ–ಮೈಲ್ ಗಳಲ್ಲೂ ಹಾಗೂ ವೆಬ್ ಸೈಟ್ ಗಳಲ್ಲೂ ಬಳಸಲು ಪರಿಣಿತರ ಸಲಹೆ ಪಡೆಯಬಹುದು.

೨. ಮಾಹಿತಿ ಕಳ್ಳತನ:

ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳಲ್ಲಿ ಕಳ್ಳತನವೆಂದರೆ ಕಂಪ್ಯೂಟರ್ ಒಳಗಿನ ''ಮಾಹಿತಿ'' ಯನ್ನು ಕದಿಯುವುದು. ಮಾಹಿತಿ ಸಾಮಾನ್ಯವಾಗಿ ಕಂಪ್ಯೂಟರ್ ನ ''ಹಾರ್ಡ್ ಡಿಸ್ಕ್'', (ಧೃಢ ಚಕ್ರ) ಒಳಗೆ ಇರುತ್ತದೆ. ಅಂತರ್ಜಾಲದ ಮಾಹಿತಿ ಕೂಡ ಅಂತರ್ಜಾಲಕ್ಕೆ ಜೋಡಣೆಯಾಗಿರುವ ಪ್ರಪಂಚದ ಯಾವುದೋ ಕಂಪ್ಯೂಟರ್ ಒಳಗಿರುತ್ತದೆ. ಈ ಮಾಹಿತಿಯನ್ನು ಮಾಹಿತಿ ಒಡೆಯನ ಒಪ್ಪಿಗೆಯಿಂದ ನಾವು ಓದಬಹುದು. ಅವನ ಒಪ್ಪಿಗೆಯಿದ್ದರೆ ಅದನ್ನು ಕಾಪಿ (ಪ್ರತಿ) ಮಾಡಿಕೊಳ್ಳಬಹುದು.

ಆದರೆ ಮಾಹಿತಿ ಒಡೆಯ ಮಾಹಿತಿಯನ್ನು ತನ್ನ ವೈಯುಕ್ತಿಕ ಉಪಯೋಗಕ್ಕಾಗಿ ಇಟ್ಟುಕೊಂಡಿದ್ದರೆ ಅದನ್ನು ಬೇರೆಯವರು ಓದುವುದಾಗಲಿ, ಪ್ರತಿ ಮಾಡಿಕೊಳ್ಳುವುದಾಗಲೀ ಅಪರಾಧವಾಗುತ್ತದೆ.

ಈ ಮಾಹಿತಿ ಕಳ್ಳತನ ಎರಡು ಬಗೆಯದೆನ್ನಬಹುದು. ಒಂದು ಕಾಪಿ ರೈಟ್ ಕಾನೂನಿನ ವ್ಯಾಪ್ತಿಯಲ್ಲಿ ಬರುವ ಮಾಹಿತಿ ದುರುಪಯೋಗ. ಇದನ್ನು ನಾವು ತದನಂತರ ವಿಶ್ಲೇಶಿಸೋಣ. ಈಗ ಕಾಪಿ ರೈಟ್ ವ್ಯಾಪ್ತಿಯ ಹೊರಗೆ ಬರುವ ಮಾಹಿತಿ ಕಳ್ಳತನದ ಬಗ್ಗೆ ವಿಚಾರ ಮಾಡೋಣ.

ಉದಾಹರಣೆಗೆ ಒಂದು ಕಂಪನಿಯನ್ನು ತೆಗೆದುಕೊಳ್ಳಿ. ಕಂಪನಿಯ ದಿನನಿತ್ಯದ ವ್ಯವಹಾರಗಳ ವಿವರಗಳು, ಅದರ ಗ್ರಾಹಕರ ವಿಳಾಸ ವಿವರಗಳು, ಮಾರಾಟ ಅಥವಾ ಕೊಳ್ಳುವಿಕೆಯ ವಿವರಗಳು, ಹಣಕಾಸು ವಿವರಗಳು, ಇವೆಲ್ಲಾ ಕಂಪನಿಯ ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿ ಕಂಡುಬರುವ ಮಾಹಿತಿಯಲ್ಲಿ ಸೇರಿರುತ್ತವೆ. ಈ ಮಾಹಿತಿ ಆ ಕಂಪನಿಗಲ್ಲದೆ ಅದೇ ರೀತಿಯ ವ್ಯವಹಾರದಲ್ಲಿರುವ ಇತರ ಕಂಪನಿಗಳಿಗೂ ಉಪಯೋಗವಾಗುತ್ತದೆ. ಆದ್ದರಿಂದ ಕಂಪನಿಯ ''ಗುಪ್ತ ಮಾಹಿತಿ''ಗೆ ಬೆಲೆ ಕೊಟ್ಟು ಕೊಳ್ಳುವ ವ್ಯಕ್ತಿಗಳು ವ್ಯವಹಾರ ವಿರೋಧಿಗಳ ಗುಂಪಿನಲ್ಲಿರುವುದು ಸಹಜ.

ಆದ್ದರಿಂದ ಕಂಪನಿಯ ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆಯ ಒಳಗೆ ನುಗ್ಗಿ ಅಲ್ಲಿರುವ ಮಾಹಿತಿಗಳನ್ನು ಪರಿಶೀಲಿಸುವುದೂ, ಬೇಕಿದ್ದರೆ ಅದನ್ನು ಕಾಪಿ ಮಾಡಿಕೊಳ್ಳುವುದೂ ಕೆಲವರು ಮಾಡುವ ಅಪರಾಧ. ಇದೇ ಮಾಹಿತಿ ಕಳ್ಳತನ.

ಕೆಲವೊಮ್ಮೆ ಕಂಪನಿಯ ಕೆಲಸಗಾರರೇ ಮಾಹಿತಿಯನ್ನು ಕದ್ದು ಇ–ಮೈಲ್ ಮೂಲಕ ಹೊರಗೆ ಕಳುಹಿಸುವ ಸಾಧ್ಯತೆ ಇರುತ್ತದೆ. ಇತ್ತೀಚೆಗಷ್ಟೆ ಮುಂಬೈ ನಲ್ಲಿ ಕಂಪನಿಯೊಂದು ತನ್ನ ಮಹಿಳಾ ಉದ್ಯೋಗಿಯ ಬಗ್ಗೆ ಈ ರೀತಿಯ ದೂರು ಕೊಟ್ಟದ್ದನ್ನು ನಾವು ನೆನಪಿಸಿಕೊಳ್ಳಬಹುದು. ಚೆನ್ನೈ ನಲ್ಲಿ ಕೂಡಾ ಕೆಲವು ತಿಂಗಳ ಹಿಂದೆ ಇಂತಹುದೇ ದೂರು ಬಂದಿತ್ತು. ಈ ಪ್ರಕರಣದಲ್ಲಿ ಒಂದು ಕಂಪನಿಯ ಕೆಲಸಗಾರ ಕಂಪನಿಯಲ್ಲಿಯೇ ತಯಾರಿಸಿದ್ದ ಒಂದು ಮುಖ್ಯ ತಂತ್ರಾಂಶ (ಸಾಫ್ಟ್ ವೇರ್) ವನ್ನು ಸಿ.ಡಿ. (ದಟ್ಟ ಚಕ್ರ) ಯಲ್ಲಿ ಕಾಪಿ ಮಾಡಿಕೊಂಡು ನಂತರ ಕಂಪನಿ ಕೆಲಸವನ್ನು ರಾಜಿನಾಮೆ ಮಾಡಿ ಬೇರೆ ಊರಿನಲ್ಲಿ ಮತ್ತೊಂದು ಕಂಪನಿಯಲ್ಲಿ ಹೆಚ್ಚಿನ ಸಂಬಳಕ್ಕೆ ಕೆಲಸಕ್ಕೆ ಸೇರಿದ. ಬಹುಶಃ ಅವನು ಕದ್ದು ತಂದಿದ್ದ ತಂತ್ರಾಂಶವನ್ನು ಆ ಕಂಪನಿಯಲ್ಲಿ ಬಳಸಲು ಅವನು ಯೋಜಿಸಿದ್ದ. ಇದರಲ್ಲಿ ಆ ಕಂಪನಿಯ ಕುಮ್ಮಕ್ಕು ಇರುವ ಸಾಧ್ಯತೆಯೂ ಇತ್ತು.

ಚೆನ್ನೈ ಕಂಪನಿ ಕೊಟ್ಟ ದೂರಿನ ಮೇಲೆ, ಅವನನ್ನು ಕರೆಸಿ ವಿಚಾರಣೆ ಮಾಡಿದಾಗ ಅವನು ತನ್ನ ತಪ್ಪೊಪ್ಪಿಕೊಂಡ. ಈ ಪ್ರಸಂಗದಲ್ಲಿ ಮಾಹಿತಿ ಕಳ್ಳತನದೊಂದಿಗೆ ಹ್ಯಾಕಿಂಗ್, ಪಿತೂರಿ, ಕಾಪಿರೈಟ್ ಉಲ್ಲಂಘನೆ ಮುಂತಾದ ಅನೇಕ ಅಪರಾಧಗಳು ಒಂದುಗೂಡಿದ್ದವು. ಈ ಕೇಸು ಮುಂದುವರೆದಿದ್ದರೆ ಮಾಹಿತಿ ಕಳ್ಳನಿಗೆ ಕನಿಷ್ಟ ೩ ವರ್ಷ ಸಜಾ ಆಗುವ ಸಾಧ್ಯತೆ ಇತ್ತು. ಕಂಪನಿ ಕೇಸನ್ನು ಮುಂದುವರೆಸದೇ ಹೋದ ಕಾರಣ ಪ್ರಕರಣ ಅಲ್ಲಿಗೇ ಮುಕ್ತಾಯ ವಾಯಿತು. ಆದರೆ ಅಪರಾಧಿ ತನ್ನ ಕೆಲಸ ಕಳೆದುಕೊಳ್ಳಬೇಕಾಯಿತು.

ಭಾರತದಲ್ಲಿರುವ ಸೈಬರ್ ಕಾನೂನಿನ ಪ್ರಕಾರ ಸೈಬರ್ ಕಳ್ಳತನದಿಂದ ನಷ್ಟ ಹೊಂದಿದವರು ವಿಶೇಷ ಕಾನೂನು ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ''ಅಡ್ಜುಡಿಕೇಟರ್'' (ಸೈಬರ್ ನಿರ್ಣಯಕಾರ) ಮೂಲಕ ಅಪರಾಧಿಗಳಿಂದ ಒಂದು ಕೋಟಿ ರೂಪಾಯಿವರೆವಿಗೆ ನಷ್ಟ ಪರಿಹಾರ ಕೇಳಬಹುದು.

೩. ಸೈಬರ್ ಕೊಲೆ :

ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳಲ್ಲಿ ಕೊಲೆಯ ಬಗ್ಗೆ ಚರ್ಚೆ ಏಕೆ ಎಂದು ಕೆಲವರಿಗೆ ಆಶ್ಚರ್ಯ ವಾಗಬಹುದು. ಆದರೆ ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಸರ್ವ ವ್ಯಾಪಿಯಾಗಿರುವ ಈ ಯುಗದಲ್ಲಿ ಕೊಲೆ ಮಾಡುವವರೂ ಕಂಪ್ಯೂಟರ್ ಬಳಸುವುದು ಸಾಮಾನ್ಯ. ಇಂಥ ಒಂದು ಪ್ರಸಂಗದಲ್ಲಿ ಅಮೆರಿಕದ ಆಸ್ಪತ್ರೆಯೊಂದರಲ್ಲಿ ಒಬ್ಬ ಕೊಲೆಗಾರ ರೋಗಿಯೊಬ್ಬನ ಬಗ್ಗೆ ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿದ್ದ ಮಾಹಿತಿಯನ್ನು ಬದಲಾಯಿಸಿ ಅವನಿಗೆ ನರ್ಸ್ ತಪ್ಪು ಔಷಧಿ ಕೊಡುವಂತೆ ಮಾಡಿ ಕೊಲೆ ಮಾಡುವುದರಲ್ಲಿ ಯಶಸ್ವಿಯಾದ ಪ್ರಕರಣ ಬೆಳಕಿಗೆ ಬಂದಿದೆ.

ಈ ಪ್ರಕರಣ ನಮಗೆ ಏನು ತೋರಿಸುತ್ತದೆಂದರೆ ಇಂದು ನಮ್ಮ ಜೀವನದ ಅನೇಕ ಜೀವನ್ಮರಣ ಪ್ರಶ್ನೆಗಳಲ್ಲಿ ಕಂಪ್ಯೂಟರ್ ಬಳಕೆಯಾಗುತ್ತಿದೆ. ಆಸ್ಪತ್ರೆಯಲ್ಲಿ ರೋಗಿಯ ತಪಾಸಣೆ ಮಾಡುವುದೂ, ತಪಾಸಣೆ ವಿವರಗಳನ್ನು ಪರಿಣಿತರಿಗೆ ಕಳುಹಿಸುವುದೂ, ಅವರು ಅದರ ಬಗ್ಗೆ ತಮ್ಮ ಅಭಿಪ್ರಾಯವನ್ನು ತಿಳಿಸುವುದೂ, ನಂತರ ಔಷಧಿ, ಚಿಕಿತ್ಸೆಯ ವಿವರಗಳನ್ನು ಸಂಗ್ರಹಿಸಿಟ್ಟು ಬೇಕಾದಾಗ ವೈದ್ಯರಿಗೆ ಒದಗಿಸುವುದೂ ಎಲ್ಲಾ ಕಂಪ್ಯೂಟರ್ ನಿಂದಲೇ ಮಾಡಲ್ಪಡುತ್ತದೆ. ಹಾಗಿದ್ದಾಗ ಯಾವುದೇ ಕಂಪ್ಯೂಟರ್ ಸರಿಯಾಗಿ ಕೆಲಸ ಮಾಡದಿದ್ದರೆ, ಅಥವಾ ಅದರ ಮಾಹಿತಿ ಸರಿಯಾಗಿ ರಕ್ಷಿಸಲಾಗದಿದ್ದರೆ ರೋಗಿಯ ಪ್ರಾಣಹರಣ ಮಾಡುವುದು ಅಪರಾಧಿಗೆ ಕಷ್ಟವಾಗಲಾರದು. ಈ ಸೈಬರ್ ಕೊಲೆಗೆ ಸಾಮಾನ್ಯ ಕಾನೂನಿನಂತೆ ಶಿಕ್ಷೆ

ವಿಧಿಸಬಹುದಲ್ಲದೆ ಸೈಬರ್ ಕಾನೂನಿನಂತೆಯೂ ಹ್ಯಾಕಿಂಗ್ ಗೆ ಇರುವ ಶಿಕ್ಷೆ ಕೊಡಬಹುದು.

ಈಗಾಗಲೇ, ತೀವ್ರವಾದಿಗಳು, ಅಂತರ್ಜಾಲದ ಮೂಲಕ ತಮ್ಮ ಅಂತರರಾಷ್ಟ್ರೀಯ ಚಟುವಟಿಕೆಗಳನ್ನು ನಡೆಸುತ್ತಿರುವುದು ತಿಳಿದಿದೆ. ಈ ತೀವ್ರವಾದಿಗಳಿಂದ ವಿಮಾನ ಚಲನವಲನ ನಿಯಂತ್ರಣ, ವಿದ್ಯುಚ್ಛಕ್ತಿ ನಿಯಂತ್ರಣ ಮುಂತಾದ ಕಡೆಗಳಲ್ಲಿನ ಕಂಪ್ಯೂಟರ್ ಗಳಿಗೆ ಆತಂಕ ಇರುವುದು ಈಗಾಗಲೇ ಸರ್ಕಾರಗಳ ಗಮನಕ್ಕೆ ಬಂದಿದ್ದು, ಸೂಚ್ಯ ರಕ್ಷಣಾ ವ್ಯವಸ್ಥೆಯನ್ನು ಸರ್ಕಾರಗಳು ಮಾಡುತ್ತಿವೆ. ಈ ರೀತಿ ಸೈಬರ್ ಅಪರಾಧಿಗಳಿಂದ ಸಾಮಾನ್ಯ ಜನ ಜೀವನಕ್ಕೆ ಹೆಚ್ಚು ಕಡಿಮೆಯಾದರೆ ಈಗಿರುವ ಕಾನೂನಿನೊಡನೆ ಸೈಬರ್ ಕಾನೂನಿನಲ್ಲಿಯೂ ಕ್ರಮ ಜರುಗಿಸಬಹುದು.

ಈ ರೀತಿಯ ರಾಷ್ಟ್ರ ವಿರೋಧಿ ಚಟುವಟಿಕೆಗಳನ್ನು ತಡೆಯುವುದಕ್ಕೆ ಭಾರತೀಯ ಸೈಬರ್ ಕಾನೂನಿನನ್ವಯ ಸರ್ಕಾರ ''ರಕ್ಷಿತ ವ್ಯವಸ್ಥೆ'' ಎಂದು ಘೋಷಿಸಲಾದ ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆಯ ಒಳಗೆ ಅತಿಕ್ರಮ ಪ್ರವೇಶ ಮಾಡುವ ಪ್ರಯತ್ನವನ್ನು ಮಾಡಿದವರಿಗೆ ೧೦ ವರ್ಷ ಸಜೆ ಕೊಡಬಹುದಾದ ಅವಕಾಶ ನೀಡಲಾಗಿದೆ.

೪. ಸೈಬರ್ ಮಾನಹಾನಿ :

ಅಂತರ್ಜಾಲದಲ್ಲಿ ಮಾನಹಾನಿ ಮೊಕದ್ದಮೆಗಳು ಭಾರತದಲ್ಲಿ ದಾಖಲಾಗುತ್ತಿರುವ ಅಪರಾಧಗಳ ಪಟ್ಟಿಯಲ್ಲಿ ಮುಂದಿದೆ ಎನ್ನ ಬಹುದು. ಮುಖ್ಯವಾಗಿ ಈ ಅಪರಾಧಗಳಿಂದ ಬಳಲುತ್ತಿರುವುದು ಅಮಾಯಕ ಯುವತಿಯರು. ಅವರಲ್ಲಿ ಅನೇಕರು ಅಂತರ್ಜಾಲವೆಂದರೇನೇಂದೂ ತಿಳಿಯದಿರುವ ಸಾಮಾನ್ಯ ಜನರು.

ಸೈಬರ್ ಮಾನಹಾನಿಯ ಒಂದು ವಿಧವೇನೆಂದರೆ, ತಮಗೆ ಆಗದ ವ್ಯಕ್ತಿಯೊಬ್ಬರ ಬಗ್ಗೆ ಅಂತರ್ಜಾಲ ಕ್ಷೇತ್ರದಲ್ಲಿ ಸುಳ್ಳು ಸುದ್ದಿಗಳನ್ನು ಬರೆಯುವುದು ಅಥವಾ ಇ–

ಮೈಲ್ ಮೂಲಕ ಇತರ ಸ್ನೇಹಿತರಿಗೆ ಕಳುಹಿಸುವುದು. ಈ ಕುತಂತ್ರದಲ್ಲಿ ಒಬ್ಬ ಮಹಿಳೆಯ ಬಗ್ಗೆ ಅವಾಚ್ಯ ಶಬ್ದಪ್ರಯೋಗ ಮಾಡುವುದು, ಅವಳು ತಾನೇ ಇತರ ಪುರುಷರನ್ನು ಆಹ್ವಾನಿಸಿ ದೂರವಾಣಿಯಲ್ಲಿ ಸಂಪರ್ಕಿಸಬೇಕೆಂದು ಬರೆಯುವುದೂ ಸೇರಿದೆ.

ಈಗ ಹಲವಾರು ವರ್ಷಗಳ ಹಿಂದೆಯೇ, ಮುಂಬೈನ ಸಿನಿಮಾ ನಟಿ ಒಬ್ಬಳು ತನ್ನ ಮುಖವನ್ನು ಬೇರಾವುದೋ ವ್ಯಕ್ತಿಯ ನಗ್ನ ಶರೀರಕ್ಕೆ ಜೋಡಿಸಿ ಅಂತರ್ಜಾಲದಲ್ಲಿ ಪ್ರಕಟಿಸಿದ್ದ ಬಗ್ಗೆ ದೂರು ಕೊಟ್ಟಿದ್ದರು. ಇದೀಗ ಈ ರೀತಿಯ ಪ್ರಕರಣಗಳು ಸರ್ವೇ ಸಾಧಾರಣವಾಗಿದೆ. ಅಲ್ಲದೆ ಇತ್ತೀಚಿಗೆ ಬಂದಿರುವ ಮೊಬೈಲ್ ಫೋನ್ ಗಳಲ್ಲಿ ಕ್ಯಾಮರಾ ಇರುವ ಪ್ರಯುಕ್ತ, ರಸ್ತೆಯಲ್ಲಿ ಹೋಗುತ್ತಿರುವ ಯಾವುದೇ ಮಹಿಳೆಯ ಮುಖವನ್ನು ಮೊಬೈಲ್ ನಲ್ಲಿ, ಸೆರೆಹಿಡಿದು ನಂತರ ದುರುಪಯೋಗ ಪಡಿಸಿಕೊಳ್ಳುವ ಸಾಧ್ಯತೆ ಹೆಚ್ಚಾಗುತ್ತಿದೆ.

ಈ ರೀತಿಯ ಮಾನ ಹಾನಿ ಪ್ರಸಂಗಗಳು ಸಾಧಾರಣವಾಗಿ ಪ್ರೇಮ ನಿರಸನ ಪ್ರಕರಣಗಳಲ್ಲೂ, ಹಾಗೂ ಕಾರ್ಯಾಲಯಗಳಲ್ಲಿ ವೈಯುಕ್ತಿಕ ವೈಷಮ್ಯಕ್ಕಾಗಿಯೂ ನಡೆದಿರುವ ಹಲವಾರು ಪ್ರಸಂಗಗಳು ಬೆಳಕಿಗೆ ಬಂದಿದೆ. ಹೆಚ್ಚಾಗಿ ಇಂತಹ ಪ್ರಸಂಗಗಳಲ್ಲಿ ಹೆಂಗಸರು ಬಲಿಯಾಗುವರಾದರೂ, ಚೆನ್ನೈನ ಒಂದು ಪ್ರತಿಷ್ಟಿತ ಕಂಪನಿಯೊಂದರಲ್ಲಿ ಕಂಪನಿಯ ಡೈರಕ್ಟರ್ ಒಬ್ಬರು ಒಬ್ಬ ಹಿರಿಯ ಮಹನೀಯ ಉದ್ಯೋಗಿಯ ಸುಳ್ಳು ಚಿತ್ರವೊಂದನ್ನು ಸೃಷ್ಟಿಸಿ ಇತರರಿಗೆ ಕಳುಹಿಸಿದ ಪ್ರಕರಣವೂ ನಡೆದಿದೆ.

ಈ ಸೈಬರ್ ಮಾನ ಹಾನಿಗೊಳಗಾದ ವ್ಯಕ್ತಿ ಭಾರತೀಯ ಅಪರಾಧ ಸಂಹಿತೆಯ ಪ್ರಕಾರ ಪೋಲೀಸರಿಗೆ ದೂರು ನೀಡುವುದಕ್ಕೆ ಕಾನೂನಿನಲ್ಲಿ ಅವಕಾಶವಿದೆ. ಆದರೆ ಈ ರೀತಿಯ ದೂರುಗಳು ನ್ಯಾಯಾಲಯದಲ್ಲಿ ನಿಲ್ಲಬೇಕಿದ್ದರೆ ಅದಕ್ಕೆ ಬೇಕಾದ ಸಾಕ್ಷಿಗಳನ್ನು ಹೊಂದಿಸಬೇಕಾದ್ದು ಅಗತ್ಯ.

೫. ಹ್ಯಾಕಿಂಗ್:

ಇದುವರೆವಿಗೂ ನಾವು ಮೋಸ, ಕೊಲೆ, ಮಾನಹಾನಿ ಮುಂತಾದ ಸಾಮಾನ್ಯ ಅಪರಾಧಗಳ ಸೈಬರ್ ಅವತಾರನನ್ನು ಅವಲೋಕಿಸಿದೆವು. ಈಗ ಸೈಬರ್ ಕ್ಷೇತ್ರದ ಮುಖ್ಯ ಅಪರಾಧಗಳಲ್ಲೊಂದಾದ ''ಹ್ಯಾಕಿಂಗ್'' ಎಂದರೆ ಏನೆಂದು ನೋಡೋಣ.

ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ಗಣಕ ಯಂತ್ರ ಮುಖ್ಯವಾಗಿ ಮಾಹಿತಿ ಸಂಗ್ರಹಣ ಮತ್ತು ಸಂಸ್ಕರಣ ಮಾಡಬಲ್ಲ ಉಪಕರಣ. (ಜೊತೆಗೆ ಕೆಲವು ಸಂಧರ್ಭದಲ್ಲಿ ಸಂಪರ್ಕ ಸಾಧನವೂ ಹೌದು). ಒಂದು ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿರುವ ಮಾಹಿತಿ ಸಾಮಾನ್ಯವಾಗಿ ಆ ಕಂಪ್ಯೂಟರ್ ನ ಮಾಲಿಕನಿಗೆ ಸೇರಿದ್ದು.

ಕಂಪ್ಯೂಟರ್ ನ ಮಾಹಿತಿಯ ಒಳಹೊಕ್ಕು ಅದನ್ನು ನೋಡುವ ಮತ್ತು ಬದಲಾಯಿಸುವ ಹಕ್ಕು ಇರುವುದೂ ಅದರ ಒಡೆಯನಿಗೆ. ವೈಯುಕ್ತಿಕ ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿ ಕಂಪ್ಯೂಟರ್ ಒಡೆತನ ಮತ್ತು ಅದರೊಳಗಿರುವ ಮಾಹಿತಿಯ ಒಡೆತನ ಒಬ್ಬರಿಗೇ ಸೇರಿರಬಹುದು.

ಕೆಲವು ಸಂಧರ್ಭಗಳಲ್ಲಿ ಒಂದು ಕಂಪ್ಯೂಟರನ್ನು ಅನೇಕರು ಉಪಯೋಗಿಸಬಹುದು. ಉದಾಹರಣೆಗೆ ಸೈಬರ್ ಕೆಫೆ ಅಥವಾ ಕೆಲಸ ಮಾಡುವ ಸ್ಥಳದಲ್ಲಿರುವ ಕಂಪ್ಯೂಟರ್. ಇಂತಹ ಹಂಚಿಕೊಂಡ ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿರುವ ಮಾಹಿತಿ ಅದನ್ನು ಯಾರು ಸೃಷ್ಟಿಸಿರುತ್ತಾರೋ ಅಥವಾ ಸಂಗ್ರಹಿಸಿರುತ್ತಾರೋ ಅವರಿಗೆ ಸೇರಿರುತ್ತದೆ ಎನ್ನಬಹುದು.

ಮಾಹಿತಿಯ ಒಡೆಯ ಅದನ್ನು ತನ್ನ ಇಷ್ಟಪ್ರಕಾರ ಇತರರಿಗೂ ಒದಗಿಸಿಕೊಡಬಹುದು. ಹಾಗೆ ಮಾಡಬೇಕಿದ್ದಲ್ಲಿ ಅವನು ಆ ಮಾಹಿತಿಯನ್ನು ಒಂದು ಫ್ಲಾಪ್ಪಿ ಅಥವಾ ಸಿ.ಡಿ.ಯಲ್ಲಿ ಕಾಪಿ ಮಾಡಿಕೊಡಬಹುದು. ಇಲ್ಲದೇ ಹೋದರೆ ಮಾಹಿತಿಯನ್ನು

ಯಾರಿಗೆ ಕೊಡಬೇಕೋ ಅವರನ್ನು ತನ್ನ ಕಂಪ್ಯೂಟರ್ ನಲ್ಲೇ ಓದಿಕೊಳ್ಳಲು ಅವಕಾಶ ಕೊಡಬಹುದು.

ಒಂದು ವೇಳೆ ಮಾಹಿತಿ ಇರುವ ಕಂಪ್ಯೂಟರ್ ಮತ್ತೊಂದು ಕಂಪ್ಯೂಟರ್ ಗೆ ಜೋಡಿಸಲ್ಪಟ್ಟಿದ್ದರೆ (ನೆಟ್ ವರ್ಕ್ ಮಾಡಲ್ಪಟ್ಟಿದ್ದರೆ), ಆ ಮತ್ತೊಂದು ಕಂಪ್ಯೂಟರ್ ನಿಂದ ನೇರವಾಗಿ ಮಾಹಿತಿಯನ್ನು ಸಂಪರ್ಕಿಸಿ ಅದನ್ನು ಓದಬಹುದು ಅಥವಾ ಪರಿವರ್ತಿಸಬಹುದು.

ಈ ರೀತಿ ಒಂದು ಕಂಪ್ಯೂಟರ್ ನ ಒಳಹೊಕ್ಕು ಅದರ ಮಾಹಿತಿ ಪ್ರದೇಶದಲ್ಲಿ ಸಂಚರಿಸುವುದಕ್ಕೆ ಆ ಮಾಹಿತಿ ಒಡೆಯನ ಅನುಮತಿ ಅಗತ್ಯ. ಅನುಮತಿಯಿಲ್ಲದೆ ಕಂಪ್ಯೂಟರ್ ನ ಒಳಹೊಕ್ಕು ಅದರಲ್ಲಿರುವ ಮಾಹಿತಿಯನ್ನು ಪರೀಕ್ಷಿಸುವುದು, ಪರಿವರ್ತಿಸುವುದು, ನಕಲು ಮಾಡಿಕೊಳ್ಳುವುದು ''ಅತಿಕ್ರಮ ಪ್ರವೇಶ'' ವಾಗುತ್ತದೆ.

ಈ ''ಮಾಹಿತಿ ಅತಿಕ್ರಮ'', ''ಹ್ಯಾಕಿಂಗ್'' ಎಂಬ ಅಪರಾಧದ ಮೂಲ. ಮಾಹಿತಿ ಅತಿಕ್ರಮದಿಂದ ಮಾಹಿತಿ ಮಾಲಿಕನಿಗೆ ಅನೇಕ ರೀತಿಯ ನಷ್ಟ ಸಂಭವಿಸುವ ಅವಕಾಶವಿರುತ್ತದೆ. ಇದರಿಂದ ಮಾಹಿತಿಯ ಗೌಪ್ಯತೆಗೆ ಭಂಗ ಬರಬಹುದು ಅಥವಾ ಮಾಹಿತಿ ಭ್ರಷ್ಟ ವಾಗಬಹುದು ಅಥವಾ ಕೆಟ್ಟುಹೋಗಬಹುದು.

ಈ ಅತಿಕ್ರಮಣ ಮತ್ತು ನಷ್ಟ ಸಂಭವ ಕೆಲವು ಬಾರಿ ಉದ್ದೇಶ ಪೂರ್ವಕ ವಾಗಿರಬಹುದು ಅಥವಾ ಇನ್ನು ಕೆಲವು ಬಾರಿ ಅನಾಹುತವಾಗಿರಬಹುದು.

ಈ ರೀತಿಯ ಸಂಭವಗಳಿಂದ ಮಾಹಿತಿ ಒಡೆಯರಿಗೆ ರಕ್ಷಣೆ ಒದಗಿಸುವ ಉದ್ದೇಶದಿಂದ ಭಾರತದಲ್ಲಿ ಮೊತ್ತ ಮೊದಲ ಬಾರಿಗೆ ''ಇನ್ಫರ್ಮೇಶನ್ ಟೆಕ್ನಾಲಜಿ ಆಕ್ಟ್ ೨೦೦೦'' ಅಥವಾ ''ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯಿದೆ'' (ಮಾತಂಕಾ–೨೦೦೦) ಯನ್ನು ಹೊರತರಲಾಯಿತು. ಈ ಕಾಯಿದೆ ಅಕ್ಟೋಬರ್ ೧೭, ೨೦೦೦ ದಿಂದ

ಜಾರಿಯಲ್ಲಿದ್ದು ಭಾರತದ ಕಾನೂನಿನಲ್ಲಿ "ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ"ದ ಅನೇಕ ವಿಚಾರಗಳಿಗೆ ಭಗವದ್ಗೀತೆಯಾಗಿದೆ ಎನ್ನಬಹುದು.

ಮಾತಂಕಾ–೨೦೦೦ ದ ೬೬ ನೇ ಸೆಕ್ಷನ್‌ನಲ್ಲಿ "ಹ್ಯಾಕಿಂಗ್" ಅಪರಾಧದ ವಿವರಣೆ ಕೊಡಲಾಗಿದೆ. ಇದರ ಪ್ರಕಾರ

> *"ಯಾವುದೇ ವ್ಯಕ್ತಿ, ಯಾವುದೇ ವಿಧಾನದಿಂದ, ಉದ್ದೇಶ ಪೂರ್ವಕವಾಗಿ ಅಥವಾ ತಾನು ಬೇರಾರಿಗಾದರೂ ನಷ್ಟವನ್ನುಂಟು ಮಾಡುವ ಸಂಭವವಿದೆಯೆಂಬ ತಿಳುವಳಿಕೆಯಿದ್ದೂ, ಕಂಪ್ಯೂಟರ್‌ನ ಒಳಗಿರುವ ಮಾಹಿತಿಯನ್ನು ನಷ್ಟಗೊಳಿಸುವುದೋ, ಅಳಿಸುವುದೋ, ಪರಿವರ್ತಿಸುವುದೋ, ಅಥವಾ ಬೇರಾವುದೇ ರೀತಿಯಲ್ಲಿ ಅದರ ಬೆಲೆ ಅಥವಾ ಉಪಯುಕ್ತತೆ ಯನ್ನು ಕಡಿತಗಳಿಸುವುದೋ, ಬಾಧೆಗೊಳಿಸುವುದೋ ಮಾಡಿದಲ್ಲಿ ಅದು "ಹ್ಯಾಕಿಂಗ್" ಎನಿಸುತ್ತದೆ. ಅಂತಹ ಅಪರಾಧಿಗೆ ೩ ವರ್ಷ ಸಜೆಯನ್ನೂ ಮತ್ತು ರೂ ೨ ಲಕ್ಷದ ವರೆಗೂ ದಂಡವನ್ನೂ ವಿಧಿಸಬಹುದು."*

ಮಾತಂಕಾ ದ ಹ್ಯಾಕಿಂಗ್ ವಿವರಣೆಯನ್ನು ಗಮನಿಸಿದರೆ, ಇದರಲ್ಲಿ ಮಾಹಿತಿ ಒಡೆಯನ ಅನುಮತಿಯ ಬಗ್ಗೆಯಾಗಲೀ ಅಥವಾ ಮಾಹಿತಿಗೆ ನಷ್ಟವುಂಟುಮಾಡುವ ವಿಧಾನದ ಬಗ್ಗೆಗಾಗಲೀ ಪ್ರಾಮುಖ್ಯತೆ ನೀಡಿಲ್ಲ. ಇದರಲ್ಲಿ ಪ್ರಾಮುಖ್ಯತೆ ಇರುವುದು, ನಷ್ಟ ಸಂಭವ ಮತ್ತು ನಷ್ಟ ಸಂಭವದ ಬಗ್ಗೆಯ ಅರಿವು ಮಾತ್ರ.

ಈ ವಿಶಾಲ ವಿವರಣೆಯ ಕಾರಣ ಬಹುತೇಕ ಕಂಪ್ಯೂಟರ್ ಅಪರಾಧಗಳನ್ನು ನಾವು ಭಾರತದಲ್ಲಿ "ಹ್ಯಾಕಿಂಗ್" ಎಂದು ಪರಿಗಣಿಸಿ ಅದರಂತೆ ಅಪರಾಧಿಗೆ ಸಜೆ/ದಂಡವನ್ನು ಕೊಡಬಹುದು. ಉದಾಹರಣೆಗೆ ಒಬ್ಬ ಕಳ್ಳ ಒಂದು ಕಂಪ್ಯೂಟರನ್ನು ಕದ್ದು ಅದರೊಳಗೆ ಇರುವ ಮಾಹಿತಿಯನ್ನು ಅಳಿಸಿ ಬೇರೆಯವರಿಗೆ ಮಾರಿದರೆ ಅದು

''ಹ್ಯಾಕಿಂಗ್'' ಎನಿಸಬಹುದು. ಒಬ್ಬ ಮಾಹಿತಿ ಸಾಫ್ಟ್‌ವೇರ್ ಉದ್ಯೋಗಿ ಕಂಪನಿಗೆ ಸೇರಿದ ಮಾಹಿತಿಯನ್ನು ಕದ್ದು ಬೇರೆಯವರಿಗೆ ಮಾರಿದರೆ ಕೂಡ ಅದು ''ಹ್ಯಾಕಿಂಗ್'' ಎಂದು ಗಣಿಸಬಹುದು. ಹಾಗೆಯೇ, ಒಂದು ಮೊಬೈಲ್ ಫೋನನ್ನು ಕದ್ದು ಅದರಲ್ಲಿರುವ ಮಾಹಿತಿಯನ್ನು ಅಳಿಸಿದರೆ ಅದು ಕೂಡ ''ಹ್ಯಾಕಿಂಗ್'' ಎನಿಸಬಹುದು.

ಯಾವುದೇ ಅಪರಾಧ ''ಹ್ಯಾಕಿಂಗ್'' ಎನಿಸಬೇಕಾದರೆ ಅದಕ್ಕೆ ಅಪರಾಧಿ ಕಂಪ್ಯೂಟರ್ ಒಳಗೆ ಪ್ರವೇಶ ಮಾಡಬೇಕೆಂಬ ಅಗತ್ಯ ಕೂಡ ಇಲ್ಲ. ಕಂಪ್ಯೂಟರ್ ನ ಹಾರ್ಡ್ ಡಿಸ್ಕನ್ನು ಬೇಕೇಂದೇ ಎತ್ತಿ ಹಾಕಿ ಅದರಲ್ಲಿರುವ ಮಾಹಿತಿಯನ್ನು ನಷ್ಟಗೊಳಿಸಿದರೆ ಕೂಡ ಅದು ''ಹ್ಯಾಕಿಂಗ್'' ಅಪರಾಧಕ್ಕೆ ಸೇರಬಹುದು.

ಆದ್ದರಿಂದ ಕಂಪ್ಯೂಟರ್ ಉಪಯೋಗಿಸುವ ಎಲ್ಲರೂ ಈ ವಿಚಾರದಲ್ಲಿ ಎಚ್ಚರದಿಂದಿರುವುದು ಸೂಕ್ತ.

''ಹ್ಯಾಕಿಂಗ್'' ಅಪರಾಧಕ್ಕೆ ಅತಿಕ್ರಮ ಪ್ರವೇಶ ಅವಶ್ಯವಲ್ಲದಿದ್ದರೂ, ಮಾಹಿತಿಯ ಅತಿಕ್ರಮ ಪ್ರವೇಶ ''ಹ್ಯಾಕಿಂಗ್''ನ ಪ್ರಮುಖ ಅಂಗವೆನ್ನಬಹುದು.

''ಹ್ಯಾಕಿಂಗ್'' ಅಲ್ಲದೆ ಯಾರಾದರೂ ಮಾಹಿತಿಯ ''ಅತಿಕ್ರಮ ಪ್ರವೇಶ'' ಮಾಡಿ ಅದರಿಂದ ನಷ್ಟ ಸಂಭವಿಸಿದಲ್ಲಿ, ಮಾತಂಕಾ–೨೦೦೦, ಸೆಕ್ಷನ್ ೪೩ ರ ಪ್ರಕಾರ ಬಾಧಿತರು ಅಪರಾಧಿಯಿಂದ ರೂ ೧ ಕೋಟಿಯವರೆಗೂ ಪರಿಹಾರಕ್ಕೆ ಹಕ್ಕುದಾರರಾಗುತ್ತಾರೆ.

ಹಾಗೇ, ಸೆಕ್ಷನ್ ೭೦ ರ ವಿಧಿಯಂತೆ ಸರ್ಕಾರ ಯಾವುದಾರರೂ ಗಣಕ ವ್ಯವಸ್ಥೆಯನ್ನು ''ರಕ್ಷಿಸಲ್ಪಟ್ಟ ವ್ಯವಸ್ಥೆ'' ಎಂದು ಘೋಷಿಸಿದ್ದರೆ ಅಂತಹ ವ್ಯವಸ್ಥೆಯ ಅತಿಕ್ರಮ ಪ್ರವೇಶದ ಪ್ರಯತ್ನ ನಡೆದರೆ (ಅಯಶಸ್ವಿಯಾದರೂ) ಅಂತಹ ಪ್ರಯತ್ನಕಾರಿಗೆ ೧೦ ವರ್ಷದ ಸಜೆ ವಿಧಿಸಲ್ಪಡಬಹುದು.

೬. ವೈರಸ್ :

ಇತ್ತೀಚಿನ ದಿನಗಳಲ್ಲಿ ಕಂಪ್ಯೂಟರ್ ವೈರಸ್‌ಗಳ (ಗಣಕ ರೋಗಾಣು) ಹಾವಳಿಯ ಬಗ್ಗೆ ನಾವು ಮಾಧ್ಯಮಗಳಲ್ಲಿ ಅನೇಕ ವಿಷಯಗಳನ್ನು ಕೇಳುತ್ತಿರುತ್ತೇವೆ.

ಮುಖ್ಯವಾಗಿ ವೈರಸ್ ಎಂದರೆ, ''ಕಂಪ್ಯೂಟರ್ ಮಾಹಿತಿಗೆ ಮಾರಕವಾಗಬಲ್ಲ ಸಾಫ್ಟ್‌ವೇರ್ ತುಣುಕು'' ಎನ್ನಬಹುದು.

ವೈರಸ್ ಕಂಪ್ಯೂಟರ್ ಒಳಗೆ ನುಗ್ಗಿದರೆ ಅದು ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿರುವ ಮಾಹಿತಿಗೆ ಅನೇಕ ರೀತಿಯಲ್ಲಿ ಹಾನಿ ಮಾಡಬಹುದು.

ಮೊದಲನೆಯದಾಗಿ ವೈರಸ್ ತನ್ನನ್ನು ತಾನೇ ಮತ್ತೆ ಮತ್ತೆ ಸೃಷ್ಟಿಸಿಕೊಂಡು, ಕಂಪ್ಯೂಟರ್ ನಲ್ಲೆಲ್ಲಾ ಆವರಿಸಿ, ಬೇರೆ ತಂತ್ರಾಂಶಗಳಿಗೆ ಜಾಗ ಕೊಡದೆ ಕಂಪ್ಯೂಟರ್ ನಿಷ್ಕ್ರಿಯಗೊಳ್ಳುವಂತೆ ಮಾಡಬಹುದು.

ಎರಡನೆಯದಾಗಿ ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿರುವ ಕಡತಗಳಲ್ಲಿ ಮಾರ್ಪಾಡುಗಳನ್ನು ಮಾಡಿ ಅಥವಾ ಅಳಿಸಿ ಹಾಕಿ ಅದು ಉಪಯೋಗಕ್ಕೆ ಬಾರದಿರುವಂತೆ ಮಾಡಬಹುದು.

ಕೆಲವು ವೈರಸ್‌ಗಳು ಕಂಪ್ಯೂಟರ್ ಜೋಡಣೆ ವ್ಯವಸ್ಥೆಯನ್ನು ಉಪಯೋಗಿಸಿಕೊಂಡು ಒಂದು ಕಂಪ್ಯೂಟರ್‌ನಿಂದ ಇನ್ನೊಂದಕ್ಕೆ ಹರಿದು ಹೋಗಬಹುದು. ಅಂತಹ ವೈರಸ್‌ಗಳಿಗೆ ''ಹುಳ'' ಎಂದು ಕರೆಯುತ್ತಾರೆ. ಈ ಹರಿದಾಟಕ್ಕೆ ಮುಖ್ಯವಾಗಿ ಈ ಗಣಕ ಹುಳಗಳು ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿರುವ ಇ-ಮೈಲ್ ಸೌಲಭ್ಯವನ್ನು ಉಪಯೋಗಿಸಿಕೊಳ್ಳುತ್ತವೆ.

ಇ–ಮೈಲ್ ಸೌಲಭ್ಯವನ್ನು ಉಪಯೋಗಿಸುವ ಸಾಮರ್ಥ್ಯವನ್ನು ಹೊಂದಿರುವ ವೈರಸ್‌ಗಳು ಕಂಪ್ಯೂಟರ್‌ನಲ್ಲಿರುವ ಯಾವುದಾದರೂ ಕಡತವನ್ನು ತೆಗೆದು ಬೇರಾರಿಗಾದರೂ ಇ–ಮೈಲ್ ಮೂಲಕ ಕಳುಹಿಸುವ ಸಾಧ್ಯತೆಗಳೂ ಉಂಟು. ಇದು ವೈರಸ್‌ಗಳು ಕೊಡುವ ಮೂರನೇ ವಿಧದ ತೊಂದರೆ.

ನಾಲ್ಕನೆ ವಿಧದ ವೈರಸ್ ತೊಂದರೆಯೇನೆಂದರೆ, ಕೆಲವು ವೈರಸ್ ಗಳು, ಗುಪ್ತಚರ ರಂತೆ ಕಂಪ್ಯೂಟರ್ ಒಳಗೆ ಕುಳಿತು ಬೇಹುಗಾರಿಕೆ ನಡೆಸುವುದು. ಕಂಪ್ಯೂಟರ್ ಬಳಕೆದಾರರು ಇ–ಮೈಲ್ ಅಥವಾ ಬ್ಯಾಂಕ್ ವ್ಯವಹಾರಗಳಿಗೆ ಉಪಯೋಗಿಸುವ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಹೊಂಚು ಹಾಕಿ ಕದ್ದು ತನ್ನ ಮಾಲಿಕನಿಗೆ ಇ–ಮೈಲ್ ಮೂಲಕ ರವಾನೆಮಾಡುವ ಈ ಬುದ್ಧಿವಂತ ವೈರಸ್ ಜಾತಿಗೆ ಸೇರಿದ ಈ ಮಾರಕ ಸಂಕೇತಗಳು ಕಂಪ್ಯೂಟರ್ ಬಳಕೆದಾರರಿಗೆ ಹೆಚ್ಚಿನ ಹಾನಿ ತರಬಲ್ಲ ವೈರಸ್‌ಗಳು. ಈ ರೀತಿ ಹೊಂಚುಹಾಕುವ ಪ್ರವೃತ್ತಿಯ ವೈರಸ್‌ಗಳನ್ನು ''ಟ್ರೋಜನ್'' ಎಂದು ಕರೆಯುತ್ತಾರೆ.

ಈ ರೀತಿ ಅನೇಕ ದುಷ್ಟ ಪ್ರವೃತ್ತಿಯನ್ನು ಹೊಂದಿರುವ ವೈರಸ್‌ಗಳು ಹೇಗೆ ಹುಟ್ಟುತ್ತವೆ? ಹೇಗೆ ಕಂಪ್ಯೂಟರ್ ಒಳಗೆ ಬರುತ್ತವೆ ಎಂಬುದು ನಾವು ತಿಳಿದಿರಬೇಕಾದ ವಿಚಾರ.

''ಗಣಕ ರೋಗಾಣು'' ಗಳು ತಾವಾಗಿಯೇ ಹುಟ್ಟುವುದಿಲ್ಲ. ಇದನ್ನು ಯಾರಾದರೂ ಕಂಪ್ಯೂಟರ್ ಸಾಫ್ಟ್‌ವೇರ್ ಬರವಣಿಗೆ ತಿಳಿದಿರುವ ವ್ಯಕ್ತಿ ಬೇಕೆಂದೇ ಸೃಷ್ಟಿಸಿ, ಇತರರಿಗೆ ತೊಂದರೆಯಾಗುವುದೆಂದು ತಿಳಿದಿದ್ದರೂ ಅದನ್ನು ಅಂತರ್ಜಾಲದ ಮೂಲಕ ಹರಿ ಬಿಡುತ್ತಾನೆಂಬುದು, ಕಟುವಾದರೂ ಸತ್ಯ. ಇದರಲ್ಲಿ ಕೆಲವರು ಯಾವುದೇ ಹಣದಾಸೆಯಿಲ್ಲದೆ ಬರಿಯ ತರಲೆ ಬುದ್ಧಿಯಿಂದ ನಡೆದುಕೊಳ್ಳುವುದೂ ದಿಟ.

ಇಂತಹವರಲ್ಲಿ ಹೆಚ್ಚಿನವರು ಜವಾಬ್ದಾರಿ ತಿಳಿಯದ ಬಾಲಕರು. ಮತ್ತೆ ಕೆಲವರು ವೈರಸ್‌ಗಳನ್ನು ಉಪಯೋಗಿಸಿ ಮಾಹಿತಿಯನ್ನು ಕದ್ದು ಅದರಿಂದ ವಂಚನೆ ಮಾಡುವ ದುರುದ್ದೇಶವುಳ್ಳ ಅಪರಾಧಿ ಮನೋಭಾವದ ವ್ಯಕ್ತಿಗಳು. ಇನ್ನು ಕೆಲವರು ತಮ್ಮದೇ ಆದ ಉದ್ದೇಶವುಳ್ಳ ತೀವ್ರವಾದಿಗಳು.

ಈ ವೈರಸ್‌ಗಳಿಂದ ಜನ ಸಾಮಾನ್ಯರಿಗೆ ಆಗುವ ತೊಂದರೆಗಳನ್ನು ಗಮನದಲ್ಲಿಟ್ಟುಕೊಂಡು ಭಾರತದ ಸೈಬರ್ ಕಾನೂನಿನ ಭಗವದ್ಗೀತೆಯಾದ ಮಾತಂಕಾ–೨೦೦೦ ದ ೪೩ ನೇ ಸೆಕ್ಷನ್ ನ ಪ್ರಕಾರ ೧ ಕೋಟಿ ಪರಿಹಾರದ ಭಾದ್ಯತೆಯನ್ನು ಈ ವೈರಸ್ ಅಪರಾಧಕ್ಕೆ ಸೂಚಿಸಲಾಗಿದೆ.

ಮಾತಂಕಾ–೨೦೦೦ ದ ಸೆಕ್ಷನ್ ೪೩ ವೈರಸ್ ಬಿಡುವ ಅಪರಾಧ ಕೇವಲ ಸಿವಿಲ್ ಅಪರಾಧದಂತಿದ್ದರೂ, ವೈರಸ್ ಪ್ರಕರಣಗಳಲ್ಲಿ ಮಾಹಿತಿಯ ನಷ್ಟವೇರ್ಪಡುವುದರಿಂದ, ಸೆಕ್ಷನ್ ೬೬ ರ ಪ್ರಕಾರ ಇದು ''ಹ್ಯಾಕಿಂಗ್'' ಅಪರಾಧವೂ ಆಗುತ್ತದೆ ಎಂಬುದು ನಾವು ಗಮನಿಸಬೇಕಾದ ವಿಚಾರ.

ಈ ವೈರಸ್‌ಗಳಿಂದ ನಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಮಾಹಿತಿಯನ್ನು ರಕ್ಷಿಸಬೇಕಾದರೆ ಆ್ಯಂಟಿ ವೈರಸ್ ಎಂದು ಕರೆಯುವ ವೈರಸ್ ನಿರೋಧಕ ತಂತ್ರಾಂಶವನ್ನು ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿ ಪ್ರತಿಷ್ಟಿಸಿ ಅದನ್ನು ದಿನ ದಿನವೂ ಅಪ್‌ಡೇಟ್ ಅಥವಾ ನವೀಕರಿಸುವುದು ಅಗತ್ಯ. ಇಲ್ಲದಿದ್ದರೆ ಸಂಕಷ್ಟ ಕಟ್ಟಿಟ್ಟ ಬುತ್ತಿ.

೭. ಅಶ್ಲೀಲತೆ

ಅಶ್ಲೀಲ ಸಾಹಿತ್ಯದ ಪ್ರಕಟಣೆ ಹಾಗೂ ಮಾರಾಟ ಈಗಾಗಲೇ ಭಾರತ ಅಪರಾಧ ಸಂಹಿತೆಯಲ್ಲಿ ಅಪರಾಧವಾಗಿ ನಮೂದಿಸಲ್ಪಟ್ಟಿದೆ. ಇದೇ ಕಾನೂನು ಈಗ ಕಂಪ್ಯೂಟರ್ ಕ್ಷೇತ್ರಕ್ಕೂ ಮಾತಂಕಾ ೨೦೦೦ ದ ಮೂಲಕ ವಿಸ್ತರಿಸಲಾಗಿದೆ. ಇದರಂತೆ

ಯಾವುದೇ ಅಶ್ಲೀಲ ವಿಚಾರ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಪತ್ರದ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಪಡಿಸುವುದೋ ಇಲ್ಲಾ ಪ್ರಸರಪಡಿಸುವುದೋ ಮಾತಂಕಾ–೨೦೦೦ ದ ಸೆಕ್ಷನ್ ೬೭ ರ ಪ್ರಕಾರ ಅಪರಾಧವಾಗುತ್ತದೆ.

ಈ ಅಪರಾಧ ಮಾಡಿದ ವ್ಯಕ್ತಿಗೆ ಮೊದಲ ಅಪರಾಧಕ್ಕೆ ೫ ವರ್ಷ ಸಜೆ ಮತ್ತು ರೂ ೧ ಲಕ್ಷ ದಂಡವನ್ನೂ, ಮತ್ತೊಮ್ಮೆ ಮಾಡಿದರೆ ೧೦ ವರ್ಷ ಸಜೆ ಹಾಗೂ ರೂ ೨ ಲಕ್ಷ ದಂಡವನ್ನೂ ವಿಧಿಸಲು ಅವಕಾಶವಿದೆ.

ಈ ಕಾನೂನಿನ ಪ್ರಕಾರ ಭಾರತದಲ್ಲಿ ಅಶ್ಲೀಲ ವೆಬ್ ಸೈಟ್ ಗಳನ್ನು ನಡೆಸುವುದು ಅಪರಾಧ ವಾಗುತ್ತದೆ. ಅಂತೆಯೇ ಅಶ್ಲೀಲ ಇ–ಮೈಲ್ ಗಳನ್ನು ಪ್ರಸಾರ ಮಾಡುವುದೂ, ಅಶ್ಲೀಲ ಚಿತ್ರಗಳನ್ನು ಮೊಬೈಲ್ ಫೋನ್‌ಗಳಿಗೆ ಅಥವಾ ಸಿ.ಡಿ. ಗಳಿಗೆ ಕಾಪಿ ಮಾಡಿ ಕೊಡುವ ವ್ಯವಹಾರ ನಡೆಸುವುದೂ ಅಪರಾಧವಾಗುತ್ತದೆ.

ಅಂತರ್ಜಾಲದಲ್ಲಿ ಅಶ್ಲೀಲತೆಗೆ ಸಂಬಂಧಪಟ್ಟ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಅಪಾರವಾಗಿವೆ. ಅಮೆರಿಕ ಮೊದಲಾದ ದೇಶಗಳಲ್ಲಿ ಬಾಲ–ಅಶ್ಲೀಲತೆ (ಚೈಲ್ಡ್ ಪೋರ್ನೋಗ್ರಫಿ) ಮಾತ್ರ ಅಪರಾಧವಾಗಿ ಪರಿಗಣಿಸಲ್ಪಡುತ್ತದೆ. ಈ ಕಾರಣದಿಂದ ಸಹಸ್ರಾರು ಅಶ್ಲೀಲ ವೆಬ್ ಸೈಟ್ ಗಳು ಹೊರದೇಶಗಳಲ್ಲಿ ರಾರಾಜಿಸುತ್ತಿವೆ. ಅಂತರ್ಜಾಲದಲ್ಲಿ ಗಡಿ ಇಲ್ಲದಿರುವುದರಿಂದ ಇತರ ದೇಶದ ಅಶ್ಲೀಲ ವೆಬ್ ಸೈಟ್ ಗಳು ಭಾರತದಲ್ಲಿಯೂ ಕಾಣಬರುತ್ತದೆ. ಅಲ್ಲದೆ ಈ ಅಶ್ಲೀಲ ವೆಬ್ ಸೈಟ್ ಗಳಲ್ಲಿರುವ ಚಿತ್ರಗಳು ಸುಲಭವಾಗಿ ಇಲ್ಲಿಯವರಿಗೂ ದೊರಕುತ್ತದೆ.

ಈ ಸೌಲಭ್ಯಗಳನ್ನು ದುರುಪಯೋಗಿಸಿಕೊಂಡು ಅನೇಕ ಕುಚೋದ್ಯಕಾರರು ತಮ್ಮ ವಿರೋಧಿಗಳ ಮಾನ ಹಾನಿ ಮಾಡುವುದಕ್ಕೆ ಅಶ್ಲೀಲ ಚಿತ್ರಗಳನ್ನು ಉಪಯೋಗಿಸುವುದು ಸಾಮಾನ್ಯವಾಗಿ ಹೋಗಿದೆ. ಇಂತಹ ಅಪರಾಧಗಳು ಮಾನ

ಹಾನಿ ಅಪರಾಧವಲ್ಲದೆ ಮಾತಂಕಾ–೨೦೦೦ ದ ಸೆಕ್ಷನ್ ೬೭ ರ ಅಪರಾಧವಾಗಿಯೂ ಗಣಿಸಲ್ಪಡುವ ಸಾಧ್ಯತೆ ಇದೆ.

ನಮ್ಮ ಯುವ ಜನಾಂಗದ ಒಳಿತಿಗಾಗಿ ಅಶ್ಲೀಲತೆಯ ಅಪರಾಧಗಳನ್ನು ತೀವ್ರವಾಗಿ ಪರಿಗಣಿಸಿ ಅಪರಾಧಿಗಳಿಗೆ ಶಿಕ್ಷೆ ಕೊಡಬೇಕಾದ ಅಗತ್ಯವನ್ನು ಒತ್ತಿ ಹೇಳಬೇಕಿಲ್ಲ. ಆದರೆ ನಿಜ ಜೀವನದಲ್ಲಿ ಅನೇಕ ಬಾರಿ ಮಾತಂಕಾ –೨೦೦೦ ದ ಸೆಕ್ಷನ್ ೬೭ ದುರುಪಯೋಗವಾಗುತ್ತಿರುವುದೂ ಉಂಟು.

ಉದಾಹರಣೆಗೆ ಈ ಸೆಕ್ಷನ್ ಅನ್ವಯ ಪೋಲೀಸಿನವರು ಆಗಾಗ್ಗೆ ಸೈಬರ್ ಕೆಫೆಗಳ ಮೇಲೆ ಕ್ರಮ ಕೈ ಗೊಳ್ಳುತ್ತಾ ಬಂದಿದ್ದಾರೆ. ಕೆಲವು ಸೈಬರ್ ಕೆಫೆ ಮಾಲೀಕರು ಅಶ್ಲೀಲ ವೆಬ್ ಸೈಟ್‌ಗಳನ್ನು ಪ್ರಚುರ ಪಡಿಸಿ ಅದರಿಂದ ಲಾಭ ಗಳಿಸುತ್ತಿರುವುದು ನಿಜ. ಆದರೆ ಒಟ್ಟಾರೆ ಸೈಬರ್ ಕೆಫೆ ಮಾಲಿಕರಲ್ಲಿ ಅನೇಕರು ನಿರಪರಾಧಿಗಳಾಗಿದ್ದರೂ ಪೋಲೀಸರಿಂದ ಕಾಡಲ್ಪಡುತ್ತಿರುವುದೂ ನಿಜ.

ಈ ವಿಷಯದಲ್ಲಿ ನಾವು ನೆನಪಿನಲ್ಲಿಡಬೇಕಾದ ಅಂಶವೇನಂದರೆ ಪ್ರಾಪ್ತ ವಯಸ್ಕನೊಬ್ಬ ಅಶ್ಲೀಲ ವೆಬ್ ಸೈಟ್ ವಿಹರಿಸುವುದು ಕಾನೂನಿನ ಪ್ರಕಾರ ಅಪರಾಧವಲ್ಲ. ಹಾಗಿರುವಾಗ ಸೈಬರ್ ಕೆಫೆಯಲ್ಲಿ ಯಾರಾದರೂ ಅಶ್ಲೀಲ ವೆಬ್ ಸೈಟ್ ನೋಡುತ್ತಿದ್ದರೆ ಸೈಬರ್ ಕೆಫೆ ಮಾಲಿಕನನ್ನು ಇದಕ್ಕೆ ಹೊಣೆ ಮಾಡುವುದೂ ಸರಿಯಲ್ಲ.

ಅದೂ ಅಲ್ಲದೆ ಮಾತಂಕ–೨೦೦೦ ದಲ್ಲಿರುವ ಸೆಕ್ಷನ್ ೭೯ ರ ಪ್ರಕಾರ ಯಾವುದೇ ‘‘ಮಾಹಿತಿ ಮಧ್ಯವರ್ತಿ’’ (ಇನ್ಫರ್ಮೇಶನ್ ಇಂಟರ್ಮೀಡಿಯರಿ) ಅಪರಾಧಗಳು ನಡೆಯದಂತೆ ಸೂಕ್ತ ಕ್ರಮಗಳನ್ನು ಕೈಗೊಂಡಿದ್ದರೆ ಮತ್ತು ಅಪರಾಧದ ಬಗ್ಗೆ ಯಾವುದೇ ಮಾಹಿತಿಯನ್ನು ಹೊಂದಿಲ್ಲದಿದ್ದರೆ ಅವನ ಮೂಲಕ ನಡೆಯುವ ಅಪರಾಧಗಳಿಗೆ ಅವನು ಹೊಣೆಯಾಗುವುದಿಲ್ಲ.

ಕರ್ನಾಟಕ ಮತ್ತು ಮುಂಬೈ ನಲ್ಲಿ ಪೋಲೀಸರು ಸೈಬರ್ ಕೆಫ಼ೆಗಳನ್ನು ನಿಯಂತ್ರಿಸಲು ಕೆಲವು ನಿರ್ದೇಶನಗಳನ್ನು ಜಾರಿಗೊಳಿಸಿದ್ದಾರೆ. ಇದರಂತೆ ಸೈಬರ್ ಕೆಫ಼ೆಗೆ ಬರುವ ಗ್ರಾಹಕರ ಬಗ್ಗೆ ಕೆಲವು ವಿವರಗಳನ್ನು ಬರೆದಿಟ್ಟುಕೊಂಡು ಅವಶ್ಯಕತೆ ಒದಗಿದಲ್ಲಿ ಅಪರಾಧ ಶೋಧನೆಗೆ ಸಹಕರಿಸಬೇಕಾದುದು ಅಗತ್ಯ.

ಅಂತೆಯೇ, ಪೋಲೀಸರು ಸೈಬರ್ ಕೆಫ಼ೆ ಮಾಲಿಕರನ್ನು ಅಶ್ಲೀಲ ವೆಬ್ ಸೈಟ್ ವೀಕ್ಷಣೆಗೆ ಹೊಣೆ ಮಾಡುವುದನ್ನು ಬಿಟ್ಟು ಅಂತಹ ಸೈಟ್ ಗಳನ್ನು ಇಂಟರ್ನೆಟ್ ಸೇವಾದಾರರ ತುದಿಯಲ್ಲೇ ಶೋಧಿಸುವ ವ್ಯವಸ್ಥೆಯನ್ನು ಮಾಡುವ ಅಗತ್ಯವಿದೆ. ಹಾಗೆಯೇ ಅಶ್ಲೀಲತೆಯ ಪ್ರಚಾರಕ್ಕೆ ಸಹಾಯ ಮಾಡುತ್ತಿರುವ ಭಾರತದಲ್ಲೇ ಇರುವ ಕೆಲವು ಪ್ರತಿಷ್ಟಿತ ಪ್ರಕಟನೆಗಳ ಬಗ್ಗೆಯೂ ಕ್ರಮ ಕೈಗೊಳ್ಳುವ ಅಗತ್ಯ ವಿದೆ.

ಹಾಗೆಯೇ ಅಶ್ಲೀಲತೆಯ ಅಪರಾಧಗಳಲ್ಲಿ ಸಿಕ್ಕಿ ಬೀಳುವ ಅಪ್ರಾಪ್ತ ವಯಸ್ಕರಿಗೆ ಸರಿಯಾದ ಮಾರ್ಗದರ್ಶನ ಮಾಡುವ ಹೊಣೆ ಶಾಲಾ ಕಾಲೇಜುಗಳ ವ್ಯವಸ್ಥಾಪಕರಿಗೂ, ತಂದೆ ತಾಯಿಯರಿಗೂ ಸೇರಿದೆ.

೮. ಸೈಬರ್ ಮುತ್ತಿಗೆ

ಸೈಬರ್ ಪ್ರದೇಶದಲ್ಲಿ ಅನೇಕ ರೀತಿಯ ವ್ಯಾಪಾರ ವ್ಯವಹಾರಗಳು ನಡೆಯುತ್ತಿರುತ್ತವೆ. ಈ ವ್ಯವಹಾರಗಳನ್ನು ನಡೆಸಲು, ಉದ್ಯಮಿಗಳು ಅದಕ್ಕೆ ಬೇಕಾದಂತಹ ವೆಬ್ ಸೈಟ್ ಗಳನ್ನು ನಡೆಸಿಕೊಂಡು ಬರುತ್ತಿರುತ್ತಾರೆ. ಈ ವೆಬ್ ಸೈಟ್ ಗಳು ನಮ್ಮ ನಿಜ ಜೀವನದಲ್ಲಿ ನಾವು ಕಾಣುವ ಅಂಗಡಿ ಗಳಂತೆ. ಇದರಲ್ಲಿ ಪದಾರ್ಥಗಳನ್ನು ಪಟ್ಟಿಮಾಡಿ ಅವುಗಳ ಬಗ್ಗೆ ಮಾಹಿತಿ ಒದಗಿಸುವ ವ್ಯವಸ್ಥೆ ಇರುತ್ತದೆ. ಇದು ನಾವು ಪೇಟೆಯಲ್ಲಿ ಕಾಣುವ ''ಷೋ ರೂಂ'' ನಂತೆ. ಇದಲ್ಲದೆ ಖರೀದಿಸಿದ ಪದಾರ್ಥಗಳಿಗೆ ಹಣ ಕೊಡುವ ''ಕ್ಯಾಷ್ ಕೌಂಟರ್'' ಕೂಡಾ ಇರುತ್ತದೆ.

ಯಾವುದೇ ವೆಬ್ ಸೈಟ್ ನಲ್ಲಿ ಕಂಡು ಬರುವ ವ್ಯಾಪಾರೀ ಸೇವೆಯನ್ನು ಪಡೆಯಬಯಸುವ ಗ್ರಾಹಕರು ಆ ನಿರ್ದಿಷ್ಟ ವೆಬ್ ಸೈಟ್ ಗೆ ಹೋಗಿ ವ್ಯವಹರಿಸಬೇಕಾಗುತ್ತದೆ. ಅನೇಕ ವೆಬ್ ಸೈಟ್ ಗಳಲ್ಲಿ ದಿನಕ್ಕೆ ಲಕ್ಷಾಂತರ ಜನ ಹಾದು ಹೋಗುತ್ತಾರೆ. ಇವರೆಲ್ಲರೂ ವ್ಯಾಪಾರ ಮಾಡಿಯೇತೀರುತ್ತಾರೆಂಬುದೇನೂ ಖಾತ್ರಿ ಇಲ್ಲ. ಆದರೂ ಅಂಗಡಿಯನ್ನು ತೆರೆದಮೇಲೆ ವ್ಯಾಪಾರಿ ಎಲ್ಲಾ ಗ್ರಾಹಕರನ್ನೂ ಬರಮಾಡಿಕೊಂಡು ಅವರಿಗೆ ಬೇಕಾದ ಮಾಹಿತಿ ಒದಗಿಸಬೇಕಾದುದು ಅಗತ್ಯ. ಆದರೆ ಒಂದು ಸಮಯದಲ್ಲಿ ಒಬ್ಬ ವ್ಯಾಪಾರಿ ಎಷ್ಟು ಜನ ಗ್ರಾಹಕರ ಅಗತ್ಯಗಳನ್ನು ಪೂರೈಸಬಲ್ಲ ಎಂಬುದಕ್ಕೆ ಮಿತಿ ಇರುವುದು ಸಹಜ. ಆ ಮಿತಿಯನ್ನು ಮೀರಿ ಗ್ರಾಹಕರು ಹರಿದು ಬಂದರೆ ವ್ಯಾಪಾರ ಅಸ್ತವ್ಯಸ್ತ ವಾಗುವುದರಲ್ಲಿ ಸಂದೇಹವಿಲ್ಲ.

"ಸೈಬರ್ ಮುತ್ತಿಗೆ" ಎಂದು ನಾವು ಹೆಸರಿಸಿರುವ ಅಪರಾಧದಲ್ಲಿ ನಡೆಯುವುದೇನೆಂದರೆ, ಒಂದು ಅಂತರ್ಜಾಲದ ವೆಬ್ ಸೈಟ್ ಗೆ ಒಂದೇ ಸಮಯದಲ್ಲಿ ಸಹಸ್ರಾರು ಅಥವಾ ಲಕ್ಷಾಂತರ ಜನರು ಪ್ರವೇಶಿಸುವ ಪ್ರಯತ್ನ ನಡೆಸಿ, ವೆಬ್ ಸೈಟ್ ವ್ಯವಸ್ಥೆ ಕುಸಿಯುವಂತೆ ಮಾಡುವುದು. ಇದಕ್ಕೆ "ಡಿನೈಯಲ್ ಆಫ್ ಸರ್ವಿಸ್" ಅಂತ ಕರೆಯುವುದು ರೂಢಿಯಲ್ಲಿದೆ.

ಸಾಮಾನ್ಯವಾಗಿ ವೆಬ್ ಸೈಟ್ ನಲ್ಲಿ ಒಂದೇ ಸಮಯದಲ್ಲಿ ಹಲವು ನೂರು ಮಂದಿ ಪ್ರವೇಶಿಸುವುದಕ್ಕೆ ತಾಂತ್ರಿಕ ವ್ಯವಸ್ಥೆಯನ್ನು ಮಾಡಲಾಗಿರುತ್ತದೆ. ಅಂತಹ ವೆಬ್ ಸೈಟ್ ನ ಶಕ್ತಿಯನ್ನು ಮೀರಿ ಹಲವು ಪಟ್ಟು ಹೆಚ್ಚು ಜನ ಪ್ರವೇಶಿಸಲು ಪ್ರಯತ್ನ ಪಟ್ಟರೆ, ಆಗ ವೆಬ್ ಸೈಟ್ ನ ತಾಂತ್ರಿಕ ವ್ಯವಸ್ಥೆ ಮುರಿದು ಬೀಳುತ್ತದೆ. ಇದರಿಂದಾಗಿ ಆ ವೆಬ್ ಸೈಟ್ ತಾತ್ಕಾಲಿಕವಾಗಿ ನಿಂತುಹೋಗಿ ವ್ಯಾಪಾರಿಗೆ ನಷ್ಟವಾಗುತ್ತದೆ.

ಈ ರೀತಿಯ ಸೈಬರ್ ಆಕ್ರಮಣ ನಡೆಸಬೇಕಾಗಿದ್ದರೆ ಒಂದೇ ಸಮಯದಲ್ಲಿ ಲಕ್ಷಾಂತರ ಕಂಪ್ಯೂಟರ್‌ಗಳು ನಿರ್ದಿಷ್ಟ ವೆಬ್ ಸೈಟ್‌ಗೆ ಪ್ರವೇಶ ಪ್ರಯತ್ನ ಮಾಡುವಂತೆ ಆಕ್ರಮಣ ಕಾರ ಮಾಡಬೇಕಾಗುತ್ತದೆ. ಆ ಸಮಯದಲ್ಲಿ ಆಕ್ರಮಣ

ಮಾಡುವ ಕಂಪ್ಯೂಟರ್ ಗಳೆಲ್ಲಾ ಅಂತರ್ಜಾಲಕ್ಕೆ ಸಂಪರ್ಕ ಹೊಂದಿರಬೇಕಾದದ್ದೂ ಅಗತ್ಯ. ಇಂತಹ ಆಕ್ರಮಣಕ್ಕೆ ಪೂರ್ವ ಸಿದ್ದತೆ ಅತ್ಯವಶ್ಯಕ.

ಈ ಪೂರ್ವ ಸಿದ್ದತೆಯಲ್ಲಿ ಆಕ್ರಮಣಕಾರ ಮೊದಲು ಮಾಡುವುದೇನೆಂದರೆ, ಅಂತರ್ಜಾಲ ಸಂಪರ್ಕ ಹೊಂದಿರುವ ಕಂಪ್ಯೂಟರ್ ಗಳಲ್ಲಿ ಸಾಧ್ಯವಾದಷ್ಟು ಕಂಪ್ಯೂಟರ್ ಗಳನ್ನು ತನ್ನ ಸೇನೆಗೆ ಸೇರ್ಪಡಿಸುವುದು. ನಂತರ ಈ ಎಲ್ಲಾ ಕಂಪ್ಯೂಟರ್ ಗಳೂ ಏಕಕಾಲಕ್ಕೆ ತನ್ನ ಗುರಿಯಾದ ವೆಬ್‌ಸೈಟ್ ಮೇಲೆ ಧಾಳಿ ನಡೆಸುವಂತೆ ಮಾಡುವುದು. ಇದಕ್ಕೆ ಅವನು ಬಳಸುವ ಸಾಧನ ನಾವು ಈ ಹಿಂದೆ ಚರ್ಚಿಸಿದ ''ಟ್ರೋಜನ್'' ಎಂಬ ವೈರಸ್ ಕುಟುಂಬಕ್ಕೆ ಸೇರಿದ ಕೀಟ.

ಈ ಟ್ರೋಜನ್, ನಿರ್ದಿಷ್ಟ ಸಮಯಕ್ಕೆ, ನಿರ್ದಿಷ್ಟ ವೆಬ್ ಸೈಟ್ ಗೆ ''ಹಲೋ, ಓ ಕಕ.ಚಚ.ಟಟ.ತತ ಎಂಬ ಹೆಸರಿನ ಕಂಪ್ಯೂಟರ್, ನಾನು ಎಂದರೆ ಕಂಪ್ಯೂಟರ್ ನಂಬರ್ ಆಆ.ಆಆ.ಇಇ.ಈಈ ನಿನ್ನೊಳಗೆ ಪ್ರವೇಶಿಸ ಬಯಸುತ್ತೇನೆ'' ಎಂಬ ಸಂದೇಶವನ್ನು ಕಳುಹಿಸುವಂತೆ ಮುಂಚೆಯೇ ಬರೆದಿಟ್ಟ ತಂತ್ರಾಂಶ ತುಣುಕನ್ನು ಹೊಂದಿರುತ್ತದೆ. (ಕಕ.ಚಚ.ಟಟ.ತತ. ಮತ್ತು ಆಆ.ಆಆ.ಇಇ.ಈಈ ಎಂಬುದು ಅಂತರ್ಜಾಲದಲ್ಲಿ ಕಂಪ್ಯೂಟರ್ ಗಳ ಗುರಿತಿಗೆ ಉಪಯೋಗಿಸುವ ಅಂಕಿಗಳು. ಇದಕ್ಕೆ ಐ.ಪಿ. ಅಡ್ರೆಸ್ಸ್ ಎಂದು ಹೆಸರು. ಈ ಐ. ಪಿ. ವಿಳಾಸದ ಬಗ್ಗೆ ಇನ್ನೂ ಹೆಚ್ಚಿನ ವಿವರವನ್ನು ಮುಂದಿನ ಪುಟಗಳಲ್ಲಿ ನೋಡೋಣ.)

ಈ ಸಂದೇಶ ಆಕ್ರಮಣಕ್ಕೊಳಗಾದ ವೆಬ್ ಸೈಟ್ ಗೆ ತಲುಪಿದಾಗ, ಅದು '' ಹಲೋ ಆಆ.ಆಆ.ಇಇ.ಈಈ, ಸರಿ ನೀನೀಗ ಬರಬಹುದು'' ಎಂಬ ಸಂದೇಶವನ್ನು ಹಿಂತಿರುಗಿಸಿ ಮುಂದಿನ ಸಮಾಚಾರಕ್ಕಾಗಿ ಕಾಯ್ದು ಕುಳಿತಿರುತ್ತದೆ. ಮುಂದಿನ ಸಂದೇಶದ ತುಣುಕು ಅದಕ್ಕೆ ಬರದಿದ್ದರೆ, ಅದು ಕಾಯುತ್ತಲೇ ಇದ್ದು ಒಂದು ಸಂದೇಶದ ದ್ವಾರ ಮುಚ್ಚಿಹೋಗುತ್ತದೆ.

ಈ ರೀತಿ ಅನೇಕ ಅರ್ಥ ಸಂದೇಶಗಳನ್ನು ಕಳುಹಿಸುವುದರಿಂದಲೂ ಅಥವಾ ಅಸಂಖ್ಯಾತ ಸಂದೇಶಗಳನ್ನು ಏಕ ಕಾಲದಲ್ಲಿ ಹರಿ ಬಿಡುವುದರಿಂದಲೂ ಆಕ್ರಮಣಕ್ಕೆ ಗುರಿಯಾದ ವೆಬ್‌ಸೈಟ್ ನಿಷ್ಕ್ರಿಯ ಗೊಳ್ಳುತ್ತದೆ.

ಈ ಅಪರಾಧ ಮಾಡುವುದು ಒಬ್ಬನಾದರೂ, ಅವನು ಹಲವಾರು ಮುಗ್ಧ ಜನರ ಕಂಪ್ಯೂಟರ್ ಗಳನ್ನು "ಟ್ರೋಜನ್" ಮೂಲಕ ತನ್ನ ಅಪರಾಧದಲ್ಲಿ ಭಾಗಿಯಾಗಿ ಮಾಡುತ್ತಾನೆ. ಆದ್ದರಿಂದ ತಮ್ಮ ಅರಿವಿಲ್ಲದೇ, ಅನೇಕ ಅಮಾಯಕರು ಈ ಅಪರಾಧದಲ್ಲಿ ಭಾಗಿಯಾಗಿ ಪ್ರಪಂಚದ ಇನ್ನಾವುದೋ ಮೂಲೆಯಲ್ಲಿರುವ ಕಂಪ್ಯೂಟರ್ ಮೇಲೆ ಧಾಳಿ ನಡೆಸುತ್ತಿರುತ್ತಾರೆಂಬುದು ಒಂದು ವಿಚಿತ್ರ ಸತ್ಯ.

ಮಾತಂಕಾ ೨೦೦೦ ಕಾನೂನಿನ ಪ್ರಕಾರ, ಈ ರೀತಿಯ ಅಪರಾಧ ಮಾಡುವವರು (ಅಥವಾ ಅಪರಾಧಕ್ಕೆ ಸಹಕರಿಸುವವರು) ೧ ಕೋಟಿ ರೂಪಾಯಿ ನಷ್ಟ ಪರಿಹಾರಕ್ಕೆ ಹೊಣೆಯಾಗುತ್ತಾರೆ.

ಈ ಸೈಬರ್ ಮುತ್ತಿಗೆ ಯ ಅಪರಾಧ ದಲ್ಲಿ ನಮಗರಿವಿಲ್ಲದೆಯೇ ಭಾಗಿಗಳಾಗುವುದನ್ನು ತಪ್ಪಿಸಲು, ತಮ್ಮ ತಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಗಳನ್ನು ಭದ್ರಪಡಿಸಿಕೊಳ್ಳಬೇಕಾದುದು ಕಂಪ್ಯೂಟರ್ ಮಾಲಿಕರೆಲ್ಲರ ಕರ್ತವ್ಯ. ಕಂಪ್ಯೂಟರ್ ಮಾಲಿಕರು ತಮ್ಮ ಬೇಜವಾಬ್ದಾರಿತನಕ್ಕೆ ಕಠಿಣ ದಂಡ ಕೊಡಬೇಕಾಗಬಹುದೆಂಬ ಅರಿವು ಮೂಡಿಸಿಕೊಳ್ಳಬೇಕಾದುದು ಕೂಡ ಅಗತ್ಯ.

೯. ಹೆಸರಿನ ಹಕ್ಕು ಉಲ್ಲಂಘನೆ

ಅಂತರ್ಜಾಲ ಪ್ರಪಂಚದಲ್ಲಿ ವ್ಯವಹರಿಸುವುದಕ್ಕೆ ಬೇಕಾದ ಒಂದು ಮುಖ್ಯ ಸಾಧನವೆಂದರೆ ಇ–ಮೈಲ್ ವಿಳಾಸ ಮತ್ತು ವೆಬ್ ಸೈಟ್ ವಿಳಾಸ. ಸರಿಯಾದ ವಿಳಾಸವಿದ್ದರೆ ಮಾತ್ರ ನಾವು ಅಂತರ್ಜಾಲದಲ್ಲಿ ಒಬ್ಬರನ್ನೊಬ್ಬರು

ಸಂಪರ್ಕಿಸಬಹುದು. ಈ ವಿಳಾಸವನ್ನು ದುರುಪಯೋಗ ಪಡಿಸಿಕೊಂಡು ಜನರನ್ನು ವಂಚಿಸುವುದು ಒಂದು ಬಗೆಯ ಅಪರಾಧ. ಹಾಗೆಯೇ ''ಹೆಸರು'' ಮತ್ತು ''ವಿಳಾಸ'', ''ಬೌದ್ಧಿಕ ಆಸ್ಥಿ'' (ಇಂಟೆಲೆಕ್ಚುಯಲ್ ಪ್ರಾಪರ್ಟಿ) ಯ ಬಗ್ಗೆಗಿನ ಕಾನೂನಿಗೆ ಸಂಬಂಧಪಟ್ಟಿವೆ. ಆದ್ದರಿಂದ ಅಂತರ್ಜಾಲದಲ್ಲೂ ನಾವು ಹೆಸರಿನ ಹಕ್ಕಿನಬಗ್ಗೆ ಇರುವ ಕಾನೂನಿನ ಬಗ್ಗೆ ಗಮನ ಹರಿಸುವುದು ಅಗತ್ಯ.

ಈಗಾಗಲೇ ತಿಳಿಸಿದಂತೆ ನೆಟ್‌ವರ್ಕ್ ನಲ್ಲಿ ಜೋಡಣೆ ಹೊಂದಿದ ಎಲ್ಲಾ ಕಂಪ್ಯೂಟರ್ ಗಳೂ ಉಪಯೋಗಿಸುವ ಗುರುತು ಐ.ಪಿ. ವಿಳಾಸ ಎಂಬ ನಾಲ್ಕು ಅಂಶ ವಿರುವ ಸಂಖ್ಯಾ ಪುಂಜ. ಉದಾಹರಣೆಗೆ ೨೦೨.೩೦.೨೫೫.೪೫ ಎಂಬುದು ಒಂದು ಐ.ಪಿ. ವಿಳಾಸ. ಅಂತರ್ಜಾಲಕ್ಕೆ ಪ್ರವೇಶಿಸುವಾಗ ನಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಗೆ ಈ ರೀತಿಯ ವಿಳಾಸ ವನ್ನು ಹಚ್ಚುವ ಕೆಲಸ ನಾವು ಉಪಯೋಗಿಸುವ ಇಂಟರ್ನೆಟ್ ಸೇವಾ ದಾರನದು. ಇದಕ್ಕಾಗಿಯೇ ನಾವು ವಿ.ಎಸ್.ಎನ್.ಎಲ್., ಸಿ.ಫ್ಟಿ., ಬಿ.ಎಸ್.ಎನ್.ಎಲ್, ಡಿಶ್‌ನೆಟ್, ಭಾರತಿ ಟೆಲ್‌ನೆಟ್, ಮುಂತಾದ ಕಂಪನಿಗಳಿಂದ ಇಂಟರ್‌ನೆಟ್ ಸೇವಾ ಸೌಲಭ್ಯವನ್ನು ಕೇಳಿ ಪಡೆಯುವುದು.

ಹೆಚ್ಚಿನ ಗ್ರಾಹಕರು ತಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಅನ್ನು ಒಂದು ಫೋನಿಗೆ ಮೋಡೆಮ್ ಲಗತ್ತಿಸಿ ಅದರಿಂದ ಇಂಟರ್ನೆಟ್ ಸೇವಾ ಸೌಲಭ್ಯಕ್ಕೆ ಸಂಪರ್ಕ ಪಡೆಯುತ್ತಾರೆ. ಇವರು ಸೇವಾದಾರನ ಸಂಪರ್ಕ ಸಾಧಿಸಿದೊಡನೆ ಅಲ್ಲಿ ಈ ಗ್ರಾಹಕನ ತತ್ಕಾಲಿಕ ಉಪಯೋಗಕ್ಕೆ ಒಂದು ಐ.ಪಿ. ವಿಳಾಸ ನಿಯೋಜಿಸಲ್ಪಡುತ್ತದೆ. ನಂತರ ಅಂತರ್ಜಾಲದಲ್ಲಿ ಈ ಗ್ರಾಹಕ ವಿಹರಿಸುವಾಗ ಈ ಐ.ಪಿ. ವಿಳಾಸವೇ ಅವನಿಗೆ ಗುರುತು ಚೀಟಿಯಾಗುತ್ತದೆ.

ಈ ತತ್ಕಾಲ ಐ.ಪಿ. ವಿಳಾಸ, ಗ್ರಾಹಕ ಅಂತರ್ಜಾಲದಿಂದ ಹೊರ ಬಂದೊಡನೆ ಮತ್ತೆ ಸೇವಾದಾರನ ಐ.ಪಿ. ವಿಳಾಸದ ಕಟ್ಟಿಗೆ ಸೇರಿಬಿಡುತ್ತದೆ. ನಂತರ ಬರುವ ಮತ್ತೊಬ್ಬ ಗ್ರಾಹಕನಿಗೆ ಇದೇ ಐ.ಪಿ. ವಿಳಾಸ ದೊರಕಿಸಿಕೊಡಲಾಗುತ್ತದೆ. ಈ ರೀತಿ ಹೆಚ್ಚಿನ

ಅಂತರ್ಜಾಲದ ಗ್ರಾಹಕರಿಗೆ ದೊರೆಯುವುದು ತತ್ಕಾಲ ಗುರುತು ಮಾತ್ರ. ಇದರಿಂದ ಅವರು ಅಂತರ್ಜಾಲದಲ್ಲಿ ವಿಹಾರ ಮಾಡಬಹುದು. ಆದರೆ ಬೇರೆಯವರು ಅವರನ್ನು ಸಂಪರ್ಕಿಸಬೇಕಿದ್ದರೆ ಒಂದು ನಿರ್ದಿಷ್ಟ ಐ.ಪಿ. ವಿಳಾಸ ಇರುವುದಿಲ್ಲ.

ವ್ಯವಹಾರಕ್ಕಾಗಲೀ ಅಥವಾ ಬೇರಾವುದೋ ಕಾರಣಕ್ಕಾಗಲೀ ವೆಬ್ ಸೈಟ್ ತೆರೆದುಕೊಂಡು ಅದಕ್ಕೆ ಗ್ರಾಹಕರನ್ನು ಬರಗೊಳಿಸಬೇಕಿದ್ದರೆ ನಮಗೆ ಖಾಯಂ ಐ.ಪಿ. ವಿಳಾಸ ಬೇಕಾಗುತ್ತದೆ. ಈ ರೀತಿಯ ಖಾಯಂ ಐ.ಪಿ. ವಿಳಾಸ ಸೌಲಭ್ಯವನ್ನು ಕೂಡಾ ಇಂಟರ್ನೆಟ್ ಸೇವಾ ದಾರರು ಒದ ಗಿಸುತ್ತಾರೆ.

ಜನ ಸಾಮಾನ್ಯರು ಈ ಐ.ಪಿ.ವಿಳಾಸ ಸಂಖ್ಯೆಯನ್ನು ಜ್ಞಾಪಕವಿಟ್ಟುಕೊಳ್ಳುವುದು ಸ್ವಲ್ಪ ಕಷ್ಟ. ಇದಕ್ಕಾಗಿ ''ಡೊಮ್ಯೈನ್ ಹೆಸರಿನ ವ್ಯವಸ್ಥೆ'' ವಾಡಿಕೆಯಲ್ಲಿದೆ. ಇದರ ಪ್ರಕಾರ ನಾವು ಯಾವುದಾದರೂ ಅಕ್ಷರ ಪುಂಜವನ್ನು ''ಡೊಮ್ಯೈನ್ ಹೆಸರು'' ಎಂದು ನೊಂದಾಯಿಸಬಹುದು. ಈ ಹೆಸರನ್ನು ನಂತರ ನಮ್ಮ ವೆಬ್ ಸೈಟ್ ಇರುವ ಕಂಪ್ಯೂಟರ್ ನ ಐ.ಪಿ. ವಿಳಾಸಕ್ಕೆ ಜೋಡಿಸಿ, ಈ ಡೊಮ್ಯೈನ್ ಹೆಸರನ್ನೇ ವಿಳಾಸವನ್ನಾಗಿ ಉಪಯೋಗಿಸಬಹುದು. ಈ ಹೆಸರನ್ನು ''ಬ್ರೌಸರ್'' ನ ಕಿಟಕಿಯಲ್ಲಿ ಬರೆದರೆ ಇಂಟರ್ನೆಟ್ ಸೇವಾದಾರರಲ್ಲಿರುವ ಮತ್ತೊಂದು ಕಂಪ್ಯೂಟರ್ ಈ ಹೆಸರನ್ನು ಐ.ಪಿ. ವಿಳಾಸಕ್ಕೆ ಬದಲಾಯಿಸಿ ವೆಬ್ ಸೈಟ್ ಇರುವ ಕಂಪ್ಯೂಟರ್ ಗೆ ಸಂಪರ್ಕ ಒದಗಿಸುತ್ತದೆ.

ಉದಾಹರಣೆಗೆ ''ಡಬ್ಲೂ ಡಬ್ಲೂ ಡಬ್ಲೂ.ನಾವಿ.ಒಆರ್ಜಿ'' (www.naavi.org) ಎಂಬುದು ವೆಬ್ ಸೈಟ್ ಒಂದರ ಹೆಸರು. ಈ ವೆಬ್ ಸೈಟ್‌ನಲ್ಲಿ ಸೈಬರ್ ಕಾನೂನಿನ ಬಗ್ಗೆ ವಿವರಗಳಿವೆ. ಈ ವಿವರಗಳು ಕಡತ ಗಳ ರೂಪದಲ್ಲಿ ಅಂತರ್ಜಾಲದಲ್ಲಿರುವ ಕಂಪ್ಯೂಟರೊಂದರ ಒಳಗೆ ಇದೆ. ಈ ಕಂಪ್ಯೂಟರ್ ನ ಐ.ಪಿ. ವಿಳಾಸ ೨೦೨.೭೧.೧೨೮.೨೧೫. ನಾವು ಬ್ರೌಸರ್ ನಲ್ಲಿ ''ಡಬ್ಲೂ ಡಬ್ಲೂ ಡಬ್ಲೂ.ನಾವಿ.ಒಆರ್ಜಿ'' ಎಂದು ಬರೆದಾಗ ಆದನ್ನು

http://www.naavi.org

ಸರಿಯಾಗಿ ಅರ್ಥೈಸಿ ೨೦೨.೭೧.೧೨೮.೨೧೫ ವಿಳಾಸ ಹೊಂದಿದ ಕಂಪ್ಯೂಟರ್ ಗೆ ಸಂಪರ್ಕ ಕೊಡುವುದು ಡೊಮೈನ್ ಹೆಸರಿನ ವ್ಯವಸ್ಥೆ.

ಈ "naavi" ಎಂಬ ಹೆಸರು ಯಾರಿಗೆ ಸೇರಿದ್ದು? ಎಂಬುದೇ "ಹೆಸರಿನ ಹಕ್ಕಿನ ಸಮಸ್ಯೆ".

ಈಗಿರುವ ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ಯಾರು ಒಂದು ಹೆಸರನ್ನು ಮೊದಲು ನೊಂದಾಯಿಸುತ್ತಾರೋ ಅವರಿಗೆ ಆ ಹೆಸರಿನ ಹಕ್ಕು ದೊರೆಯುತ್ತದೆ. ನೊಂದಣಿದಾರರು ಇದಕ್ಕೆ ಬೇಕಾದ ನೊಂದಣಿ ಶುಲ್ಕವನ್ನು "ರಿಜಿಸ್ಟ್ರಾರ್ ಗೆ" ಕಟ್ಟಬೇಕು ಹಾಗೂ ಕಾಲ ಕಾಲಕ್ಕೆ ಪುನರ್ಜೀವಿತಗೊಳಿಸಬೇಕು. ಈ "ರಿಜಿಸ್ಟ್ರಾರ್ ಗಳು", "ಐಕಾನ್" ಎಂಬ ಅಂತರರಾಷ್ಟ್ರೀಯ ಸಂಸ್ಥೆಯ ನಿರ್ಬಂಧಕ್ಕೆ ಒಳಪಟ್ಟಿರುತ್ತವೆ ಮತ್ತು ಅದರಿಂದ ಪರವಾನಿಗೆ ಪಡೆದಿರುತ್ತವೆ. ಸಧ್ಯಕ್ಕೆ ಈ ವ್ಯವಸ್ಥೆ ಯಾವುದೇ ಸರಕಾರೀ ಸ್ವಾಮ್ಯಕ್ಕೂ ಒಳಪಟ್ಟಿಲ್ಲದೆ ಸ್ವಯಂ ನಿಯಂತ್ರಿತ ಸಂಸ್ಥೆಯಾಗಿದೆ. (ಇದೀಗ ವಿಶ್ವ ಸಂಸ್ಥೆಯ ಚೌಕಟ್ಟಿನಲ್ಲಿ ಒಂದು ಹೊಸ ಅಂತರ್ಜಾಲ ನಿಯಂತ್ರಣ ವ್ಯವಸ್ಥೆ ಹುಟ್ಟಿಕೊಂಡಿದೆ. ಬಹುಶಃ ೨೦೦೫ ರ ವೇಳೆಗೆ ಈ ವ್ಯವಸ್ಥೆ ಜಾರಿಗೆ ಬರಬಹುದಾದ ಸಾಧ್ಯತೆ ಇದೆ).

ಇಂದಿನ ನೊಂದಾವಣೆ ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ಕೆಲವು ಬಾರಿ ನೊಂದಾವಣೆಯಾದ ಹೆಸರು ಬೇರಾವುದೋ ಹೆಸರಾಂತ ಪದಾರ್ಥದ ಹೆಸರಾಗುವ ಸಾಧ್ಯತೆ ಇರುತ್ತದೆ. ಉದಾಹರಣೆಗೆ ಯಾರಾದರೂ arial.com ಎಂದು ಹೆಸರನ್ನು ದಾಖಲಿಸುತ್ತಾರೆಂದು ಇಟ್ಟುಕೊಳ್ಳೋಣ. ಇದು "ಏರಿಯಲ್" ಹೆಸರಿನ ಸೋಪಿನ ಪುಡಿಯ ಹೆಸರನ್ನು ಹೋಲುವುದರಿಂದ, ಜನ ಸಾಮಾನ್ಯರು ಮೋಸಗೊಳ್ಳುವ ಅವಕಾಶವಿರುತ್ತದೆ. ಹಾಗೆ "ಏರಿಯಲ್" ಎಂಬ ಹೆಸರನ್ನು "ಟ್ರೇಡ್ ಮಾರ್ಕ್" ಖಾಯಿದೆಯನ್ವಯ ನೊಂದಾಯಿಸಿದವರ ಹಕ್ಕು ಉಲ್ಲಂಘನೆ ಆಗುತ್ತದೆ.

http://www.naavi.org

"ಟ್ರೇಡ್ ಮಾರ್ಕ್" ಖಾಯಿದೆ ಮತ್ತು "ಡೊಮೈನ್ ಹೆಸರಿನ" ಸಂಘರ್ಷ ಅಂತರ್ಜಾಲ ಕ್ಷೇತ್ರದಲ್ಲಿ ದೊಡ್ಡ ಸಮಸ್ಯೆ. ಏಕೆಂದರೆ "ಟ್ರೇಡ್ ಮಾರ್ಕ್" ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ಪ್ರತಿ ದೇಶವೂ ತನ್ನ ಭೌಗೋಳಿಕ ವ್ಯಾಪ್ತಿಯೊಳಗೆ ವಿವಿಧ ವಸ್ತುಗಳಿಗೆ ಪ್ರತ್ಯೇಕವಾಗಿ ಟ್ರೇಡ್ ಮಾರ್ಕ್ ನೊಂದಾಯಿಸುವ ಸೌಲಭ್ಯ ವನ್ನು ಕಾನೂನಿನ ಪ್ರಕಾರ ಒದಗಿಸಿವೆ. ಟ್ರೇಡ್ ಮಾರ್ಕ್ ಹಕ್ಕು ಉಲ್ಲಂಘಿಸಲ್ಪಟ್ಟರೆ ದಂಡ ವಿಧಿಸುವ ವ್ಯವಸ್ಥೆ ಕಾನೂನಿನಲ್ಲಿದೆ. ಈ ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ಒಂದೇ ಹೆಸರು ಬೇರೆ ಬೇರೆ ವಸ್ತುವಿಗಾಗಲಿ ಅಥವಾ ಬೇರೆ ಪ್ರದೇಶದಲ್ಲಾಗಲೀ ಟ್ರೇಡ್ ಮಾರ್ಕ್ ಆಗಿ ಉಪಯೋಗವಾಗುವುದಕ್ಕೆ ಅವಕಾಶವಿತ್ತು.

ಅಂತರ್ಜಾಲ ಹುಟ್ಟಿದ ಮೇಲೆ ಭೌಗೋಳಿಕ ಮಿತಿಗೆ ಅರ್ಥವಿಲ್ಲದಂತಾಗಿದೆ. ಇದರಿಂದ ಒಂದು ಪ್ರದೇಶದಲ್ಲಿ ಟ್ರೇಡ್ ಮಾರ್ಕ್ ಆಗಿ ನೊಂದಾವಣೆಯಾದ ಹೆಸರನ್ನು ಪ್ರಪಂಚದಲ್ಲಿ ಬೇರೆ ಯಾರಾದರೂ ಡೊಮೈನ್ ಹೆಸರಾಗಿ ನೊಂದಾಯಿಸಿದರೆ, ಟ್ರೇಡ್ ಮಾರ್ಕ್ ಹಕ್ಕು ಉಲ್ಲಂಘನೆಯ ಪ್ರಶ್ನೆ ಏಳುತ್ತದೆ. ಕೆಲವು ಬಾರಿ ಈ ರೀತಿಯ ಸಂಘರ್ಷ ಇಬ್ಬರು ಸಮಾನ ಹಕ್ಕುದಾರರ ನಡುವೆಯೂ ಏಳಬಹುದು.

ಈ ರೀತಿಯ ಹಕ್ಕು ಚ್ಯುತಿ ಪ್ರಶ್ನೆಯನ್ನು ಪರಿಹರಿಸಲು ಡೊಮೈನ್ ಹೆಸರನ್ನು ನೊಂದಾಯಿಸುವಾಗ "ಆರ್ಬಿಟ್ರೇಶನ್" (ಪಂಚಾಯತಿ) ವ್ಯವಸ್ಥೆಯೊಂದಕ್ಕೆ ಒಳಪಡಲು ಒಪ್ಪಿಗೆ ಪಡೆಯಲಾಗುತ್ತದೆ. ಅದರಂತೆ ಹೆಚ್ಚಿನ ಡೊಮೈನ್ ಹೆಸರಿನ ಸಮಸ್ಯೆಗಳು ಆರ್ಬಿಟ್ರೇಶನ್ ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ಪರಿಹರಿಸಿಕೊಳ್ಳಲಾಗುತ್ತದೆ.

ಮಾತಂಕಾ–೨೦೦೦ ಖಾಯಿದೆಯಲ್ಲಿ ಈ ಹೆಸರಿನ ಕಗ್ಗಂಟಿನ ಬಗ್ಗೆ ಪ್ರಸ್ತಾಪವಿಲ್ಲ. ಆದ್ದರಿಂದ ಆರ್‌ಬಿಟ್ರೇಶನ್ ವ್ಯವಸ್ಥೆ ಡೊಮೈನ್ ಹೆಸರಿನ ಸಮಸ್ಯೆಗಳಲ್ಲಿ ಪ್ರಾಮುಖ್ಯತೆಯನ್ನು ಪಡೆಯುತ್ತದೆ.

ಡೊಮೈನ್ ಹೆಸರಿನ ಸಮಸ್ಯೆ ಬರಿ ಟ್ರೇಡ್ ಮಾರ್ಕ್ ಗಲ್ಲದೆ ಹೆಸರುವಾಸಿ ಜನಗಳ ವೈಯುಕ್ತಿಕ ಹೆಸರುಗಳಿಗೂ ಅನ್ವಯಪಡಿಸಲಾದ ಅನೇಕ ಉದಾಹರಣೆಗಳು ಇದೆ. ಇದರಂತೆ ಭಾರತದಲ್ಲಿ ಬಹುಶಃ "www.sachin.com" ಎಂಬ ಹೆಸರನ್ನು ಸಚಿನ್ ತೆನ್‌ಡುಲ್ಕರ್ ಅಲ್ಲದೆ ಬೇರೆ ಯಾರಾದರೂ ಉಪಯೋಗಿಸಿದರೆ ಅದು ಹಕ್ಕು ಉಲ್ಲಂಘನೆ ಯಾಗಬಹುದು.

ಇದುವರೆಗೂ ಈ ಸಮಸ್ಯೆ ಡೊಮೈನ್ ಹೆಸರಿಗೆ ಮಾತ್ರ ಸೀಮಿತವಾಗಿದ್ದು ಇ–ಮೈಲ್ ವ್ಯವಹಾರಕ್ಕೆ ವಿಸ್ತರಿಸಲ್ಪಟ್ಟಿಲ್ಲ ಎಂಬುದು ನೆಮ್ಮದಿಯ ಸಂಗತಿ. ಇಲ್ಲದಿದ್ದರೆ ಜನ ಸಾಮಾನ್ಯರಿಗೆ ಇ–ಮೈಲ್ ವಿಳಾಸ ಸಿಕ್ಕುವುದೇ ಕಷ್ಟವಾಗುತ್ತಿತ್ತು.

ಡೊಮೈನ್ ಹೆಸರಿನ ಸಮಸ್ಯೆಯೂ ಇನ್ನೂ ಪೂರ್ಣವಾಗಿ ಪರಿಹಾರವಾಗಿಲ್ಲವೆಂದೇ ಹೇಳಬಹುದು. ಇದೀಗ ಇಂಗ್ಲಿಷ್ ಅಲ್ಲದೆ ಬೇರೆ ಭಾಷೆಯಲ್ಲೂ ಡೊಮೈನ್ ಹೆಸರುಗಳನ್ನು ನೊಂದಾಯಿಸುವ ವ್ಯವಸ್ಥೆ ಬರುತ್ತಾ ಇದೆ. ಹಾಗೆ ಬಂದಾಗ ಒಂದೇ ಅರ್ಥ ಬರುವ ಬೇರೆ ಬೇರೆ ಭಾಷೆಯ ಹೆಸರುಗಳು ಸಮಸ್ಯೆಗಳನ್ನುಂಟು ಮಾಡಬಹುದು.

ಡೊಮೈನ್ ಹೆಸರಿನ ಹಕ್ಕು ಉಲ್ಲಂಘನೆ ಇಲ್ಲಿ ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳ ಪಟ್ಟಿಯಲ್ಲಿ ಸೇರಿಸಲ್ಪಟ್ಟಿದ್ದರೂ ಇದರ ಬಗ್ಗೆ ಇನ್ನೂ ವಿಶಾಲ ಚಿಂತನೆ ಅಗತ್ಯವಿದೆಯೆನ್ನಬಹುದು. ಈ ಸಮಸ್ಯೆಯ ಪರಿಹಾರಕ್ಕೆ ಸ್ವಲ್ಪಮಟ್ಟಿಗೆ ಸಹಾಯವಾಗುವಂತೆ www.verify4lookalikes.com ಎಂಬ ವೆಬ್ ಸೈಟ್ ನಲ್ಲಿ ವಿಶಿಷ್ಟ ರೀತಿಯ ಸೇವೆಯೊಂದನ್ನು ಒದಗಿಸಿಕೊಡಲಾಗುತ್ತಿದೆ. ಈ ಸೇವೆ ಅಂತರ್ಜಾಲ ಸಮಾಜದಲ್ಲಿ ಒಪ್ಪಿಗೆಯಾದಲ್ಲಿ ಡೊಮೈನ್ ಹೆಸರಿನ ಸಮಸ್ಯೆ ಬಗೆಹರಿಯುವ ಸಾಧ್ಯತೆ ಇದೆ.

೧೦. ಕಾಪಿ ರೈಟ್

ಕಾಪಿ ರೈಟ್ ಉಲ್ಲಂಘನೆ ಮತ್ತೊಂದು ''ಭೌದ್ಧಿಕ ಆಸ್ಥಿ'' ಹಕ್ಕಿಗೆ ಸಂಬಂಧ ಪಟ್ಟ ವಿಷಯ. ಇದೂ ಕೂಡಾ ಮಾತಂಕಾ–೨೦೦೦ ಖಾಯಿದೆಯಲ್ಲಿ ಪ್ರಸ್ತಾಪ ಪಟ್ಟಿಲ್ಲ. ಆದರೆ ಈಗಾಗಲೇ ಇರುವ ಕಾಪಿರೈಟ್ ಖಾಯಿದೆಯಲ್ಲಿಯೇ ''ಕಂಪ್ಯೂಟರ್ ನಿಂದ ರಚಿತವಾದ'' ಬರವಣಿಗೆಗಳಿಗೂ ಆದು ಅನ್ವಯವಾಗುವಂತೆ ಉಲ್ಲೇಖವಾಗಿರುವುದರಿಂದ, ಕಾಪಿರೈಟ್ ಖಾಯಿದೆಯಲ್ಲಿರುವ ಎಲ್ಲಾ ಅಂಶಗಳೂ ಅಂತರ್ಜಾಲದಲ್ಲಿರುವ ಅಥವಾ ಬಿಡಿ ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿರುವ ದಾಖಲೆಗಳಿಗೆಲ್ಲಾ ಅನ್ವಯವಾಗುತ್ತದೆ.

ಕಾಪಿರೈಟ್ ಖಾಯಿದೆಯ ಮುಖ್ಯ ಅಂಶವೇನೆಂದರೆ, ಯಾವುದೇ ಸಾಹಿತ್ಯ ವಸ್ತುವಿನಲ್ಲೂ ಅದರ ರಚನಕಾರನಿಗೆ ಮೂಲವಾದ ಹಕ್ಕು ಇರುತ್ತದೆ. ಆ ಕೃತಿಯನ್ನು ಬೇರಾರೂ ಅವನ ಅಪ್ಪಣೆಯಿಲ್ಲದೆ ಮರು ಪ್ರತಿ ಮಾಡಲಾಗುವುದಿಲ್ಲ. ಹಾಗೆ ಮಾಡಿದರೆ ರಚನಕಾರ ಸೂಕ್ತ ಕ್ರಮ ಜರುಗಿಸಿ ನಷ್ಟ ಪರಿಹಾರ ಕೇಳಬಹುದು.

ಹಾಗೆಯೇ ರಚನಕಾರ ಒಪ್ಪಿದಲ್ಲಿ ರಾಯಲ್ಟಿ ಪಡೆದು ರಚನೆಯ ಹಕ್ಕನ್ನು ಇನ್ನೊಬ್ಬರಿಗೆ ರವಾನಿಸಬಹುದು.

ಇದೇ ಕಾನೂನು ಅಂತರ್ಜಾಲದ ವೆಬ್ ಸೈಟ್‌ಗಳಲ್ಲಿರುವ ಬರವಣಿಗೆ ಗಳಿಗೂ, ಚಿತ್ರ ಮತ್ತು ಹಾಡು ಮುಂತಾದ ವಸ್ತುಗಳಿಗೂ ಕಂಪ್ಯೂಟರ್ ಸಾಫ್ಟ್‌ವೇರ್ ಗೂ ಅನ್ವಯವಾಗುತ್ತದೆ. ಸಾಫ್ಟ್ ವೇರ್ ಅಥವಾ ಯಾವುದೇ ಗಣಕ ಪತ್ರದ ರಚನಕಾರನ ಕಾಪಿ ರೈಟನ್ನು ಉಲ್ಲಂಘಿಸುವುದು ಅಂತರ್ಜಾಲದ ಅಪರಾಧಗಳ ಪಟ್ಟಿಯಲ್ಲಿ ಸೇರಿದೆ.

ಡೊಮೈನ್ ಹೆಸರಿನ ಸಮಸ್ಯೆಯಲ್ಲಿರುವಂತೆ, ಸೈಬರ್ ಕ್ಷೇತ್ರದ ಕಾಪಿ ರೈಟ್ ವಿಚಾರದಲ್ಲೂ ಅನೇಕ ತಾಂತ್ರಿಕ ಅಡಚಣೆಗಳಿವೆ. ಇದರ ಬಗ್ಗೆ ಕೂಡಾ ಹೆಚ್ಚಿನ ವಿಚಾರ ಮಂಥನ ಅಗತ್ಯ ವೆನ್ನ ಬಹುದು.

೧೧. ಪೇಟೆಂಟ್

ಕಂಪ್ಯೂಟರ್ ಸಾಫ್ಟ್‌ವೇರ್ ನ ರಚನಕಾರನಿಗೆ ಕಾಪಿ ರೈಟ್ ಅಧಿಕಾರವಲ್ಲದೆ ''ಪೇಟ್‌ಂಟ್'' ಅಧಿಕಾರವೂ ಇರುತ್ತದೆ. ಈ ಅಧಿಕಾರದಲ್ಲಿ ಯಾವುದೇ ಹೊಸ, ಉಪಯುಕ್ತ ರಚನೆಯೊಂದಕ್ಕೆ ನೊಂದಾವಣೆ ಮೂಲಕ ನಿರ್ಧಿಷ್ಟ ಅವಧಿಯ ವರೆಗೆ ವಿಶೇಷ ಹಕ್ಕನ್ನು ನೀಡುವ ಕಾನೂನು ವ್ಯವಸ್ಥೆ ಇದೆ.

ಈ ವಿಶೇಷ ಹಕ್ಕಿನ ಪ್ರಕಾರ ಸಂಶೋಧಕನಲ್ಲದೆ ಬೇರೆ ಯಾರಾದರೂ ಆ ಸಂಶೋಧನೆಯನ್ನು ಉಪಯೋಗ ಪಡಿಸಿಕೊಳ್ಳಬೇಕಿದ್ದರೆ ಅವರು ಸಂಶೋಧಕನಿಗೆ ರಾಯಲ್ಟಿ ಕೊಟ್ಟು ಹಕ್ಕನ್ನು ಕೊಂಡುಕೊಳ್ಳಬೇಕಾಗುತ್ತದೆ.

ಈ ರೀತಿ ಹಕ್ಕನ್ನು ಕೊಂಡುಕೊಳ್ಳದೆ ಸಂಶೋಧನೆಯನ್ನು ಉಪಯೋಗಿಸಿದ್ದೇ ಆದರೆ ಅದು ಅಪರಾಧವೆಂದು ಪರಿಗಣಿಸಲ್ಪಟ್ಟು ಅಪರಾಧಿ ನಷ್ಟ ಪರಿಹಾರ ಕೊಡಬೇಕಾಗುತ್ತದೆ.

ಮಾತಂಕಾ–೨೦೦೦ ದಲ್ಲಿ ಪೇಟೆಂಟ್ ಬಗ್ಗೆ ಉಲ್ಲೇಖವಿಲ್ಲ. ಇದು ಒಂದು ಅಂತರ ರಾಷ್ಟ್ರೀಯ ಕಾನೂನು ವ್ಯವಸ್ಥೆ. ಇದಕ್ಕೆ ಭಾರತದಲ್ಲಿ ವಿಶೇಷ ಖಾಯಿದೆ ಇದೆ. ಅಂತರ್ಜಾಲದಲ್ಲಿ ವ್ಯಾಪಾರ ವಹಿವಾಟುಗಳನ್ನು ನಡೆಸುವವರು ಈ ಕಾನೂನಿನ ಬಗ್ಗೆ ಎಚ್ಚರ ವಹಿಸುವುದು ಉತ್ತಮ.

೧೨: ಸ್ಪ್ಯಾಮ್ (ಇ–ಮೈಲ್ ಹೊಡೆತ)

ಅಂತರ್ಜಾಲ ಪ್ರಾರಂಭವಾದಾಗಿನಿಂದ, ಇ–ಮೈಲ್ ಮೂಲಕ ಮಾರಾಟ ಸಂದೇಶಗಳನ್ನು ಕಳುಹಿಸುವುದು ಖರ್ಚಿಲ್ಲದೆ ಸಹಸ್ರಾರು ಗ್ರಾಹಕರನ್ನು ಸಂಪರ್ಕಿಸುವ ವಿಧಾನವಾಗಿ ಬೆಳೆದು ಬಂತು. ಆದರೆ ಬರು ಬರುತ್ತಾ, ಇದು ಇ–ಮೈಲ್ ಗ್ರಾಹಕರಿಗೆ ತಲೆನೋವಾಗಿ ಪರಿಣಮಿಸಿದೆ. ಏಕೆಂದರೆ ಇಂದು ನಮ್ಮ ಅನುಮತಿ ಇಲ್ಲದೆ ನಮಗೆ ಬಂದು ಸೇರುವ ಇ–ಮೈಲ್ ನಮ್ಮ ಒಟ್ಟು ಇ–ಮೈಲ್ ಗಳಲ್ಲಿ ಸುಮಾರು ಶೇಖಡಾ ೯೦ ರಷ್ಟಕ್ಕೆ ಏರಿದೆ. ಇದರಿಂದ ನಮ್ಮ ಇ–ಮೈಲ್ ಪೆಟ್ಟಿಗೆ ಗಳು ಭರ್ತಿಯಾಗಿ ನಮಗೆ ಬರಬೇಕಾದ ಇ–ಮೈಲ್ ಗಳು ಹಿಂತಿರುಗುವ ಸಾಧ್ಯತೆ ಇದೆ. ಅಲ್ಲದೆ ಹೆಚ್ಚಿನ ಇ–ಮೈಲ್ ಗಳು ಅಶ್ಲೀಲ ವಿಚಾರಗಳ ಪ್ರಚಾರಕ್ಕಾಗಿಯೂ, ವೈರಸ್ ಪ್ರಸರಣಕ್ಕೂ ಉಪಯೋಗಿಸಲ್ಪಡುತ್ತಿದೆ. ಈ ರೀತಿ ನಮ್ಮ ಅನುಮತಿಯಿಲ್ಲದೆ ಬರುವ ಇ–ಮೈಲ್ ಗೆ ಸ್ಪ್ಯಾಮ್ (spam) ಎಂದು ಕರೆಯುತ್ತಾರೆ.

ಈ ಇ–ಮೈಲ್ ಹೊಡೆತದಿಂದ ಆಗುವ ದುಷ್ಪರಿಣಾಮಗಳನ್ನು ಗುರುತಿಸಿ ಅಮೆರಿಕ ದಂತಹ ಕೆಲವು ದೇಶಗಳಲ್ಲಿ ಇದನ್ನು ಕಾನೂನು ಬಾಹಿರವೆಂದು ಘೋಶಿಸಲಾಗಿದೆ.

ಭಾರತದ ಕಾನೂನಿನಲ್ಲಿ ಇನ್ನೂ ಇ–ಮೈಲ್ ಹೊಡೆತವನ್ನು ಪ್ರತ್ಯೇಕ ಅಪರಾಧವಾಗಿ ಪರಿಗಣಿಸಿಲ್ಲ. ಆದರೆ ಈ ಇ–ಮೈಲ್ ಗಳಿಂದ ನಮ್ಮ ಅಪರಾಧ ಸಂಹಿತೆಯಲ್ಲಿರುವ ಅಪರಾಧಗಳಾವುದಾದರೂ ನಡೆದರೆ ಅದಕ್ಕೆ ಶಿಕ್ಷೆ ಈಗಾಗಲೇ ಇದೆ. ಪದೇ ಪದೇ ಇ–ಮೈಲ್ ಗಳನ್ನು ಕಳುಹಿಸಿ ಮನ ನೆಮ್ಮದಿಯನ್ನು ಹಾಳು ಮಾಡಿದರೆ ಅದಕ್ಕೆ ಅಪರಾಧ ಸಂಹಿತೆಯಲ್ಲಿ ಕ್ರಮ ಕೈಗೊಳ್ಳಬಹುದು. ಹಾಗೆಯೇ ವೈರಸ್ ಮತ್ತು ಅಶ್ಲೀಲ ಮೈಲ್ ಗಳ ಬಗ್ಗೆಯೂ ಕ್ರಮ ಕೈಗೊಳ್ಳಬಹುದು.

ಆದರೂ ಎಲ್ಲಾ ಸಮಯದಲ್ಲೂ ಇ–ಮೈಲ್ ಹೊಡೆತಕ್ಕೆ ಅಪರಾಧ ಸಂಹಿತೆ ಕೊಡುವ ರಕ್ಷಣೆ ಸಾಕಾಗುವುದಿಲ್ಲವೆನ್ನಬಹುದು. ಇದೀಗ ಇದಕ್ಕೆ ಪ್ರತ್ಯೇಕ ಕಾನೂನು ತರುವ ಬಗ್ಗೆ ಕೇಂದ್ರ ಸರ್ಕಾರ ಕ್ರಮ ತೆಗೆದುಕೊಳ್ಳುತ್ತಿದೆಯೆಂಬ ಸುದ್ದಿಯಿದೆ.

೧೩: ವ್ಯಕ್ತಿಗತ ವಿಷಯ ರಕ್ಷಣೆ

ಇತ್ತೀಚಿನ ದಿನಗಳಲ್ಲಿ ಹೆಚ್ಚಿನ ಪ್ರಾಮುಖ್ಯತೆ ಪಡೆದುಕೊಂಡಿರುವುದು ವ್ಯಕ್ತಿಗತ ಸ್ವಾತಂತ್ರ್ಯ ಮತ್ತು ಅದರೊಡನೆ ವ್ಯಕ್ತಿಗತ ವಿಷಯದ ರಕ್ಷಣೆ. ಈ ಕಂಪ್ಯೂಟರ್ ಯುಗದಲ್ಲಿ ನಮ್ಮ ಹೆಸರು, ವಯಸ್ಸಿನಿಂದ ಹಿಡಿದು, ನಮ್ಮ ಜನ್ಮ ದಿವಸ, ನಮ್ಮ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಿವರ, ನಮ್ಮ ಆರೋಗ್ಯ, ಅನಾರೋಗ್ಯದ ವಿಷಯ, ಕೆಲಸದ ವಿಷಯ ಮುಂತಾದುವೆಲ್ಲಾ ಇಂದು ಅಂತರ್ಜಾಲದಲ್ಲಿ ಸೇರಿಹೋಗಿವೆ. ಇದರಲ್ಲಿ ವೈಯುಕ್ತಿಕ ವಿಷಯಗಳು ಗುಟ್ಟಾಗಿರಬೇಕಾದುದು ಸಾಮಾನ್ಯ ಅಭಿಲಾಷೆ. ವೈಯುಕ್ತಿಕ ವಿಷಯಗಳು ಎಷ್ಟು ಬೇಕೋ ಅಷ್ಟು ಮಾತ್ರ ಬಹಿರಂಗ ಮಾಡಬೇಕೆಂಬುದು, ವಿಶ್ವ ಸಂಸ್ಥೆಯ ಮಾನವೀಯ ಹಕ್ಕುಗಳಲ್ಲಿರುವ ಹಾಗೂ ನಮ್ಮ ಭಾರತದ ಸಂವಿಧಾನದಲ್ಲಿರುವ ಮೂಲಭೂತ ಹಕ್ಕು.

ಆದ್ದರಿಂದ ಯಾವುದೇ ವ್ಯಕ್ತಿ ಈ ವ್ಯಕ್ತಿಗತ ಹಕ್ಕಿಗೆ ಚ್ಯುತಿ ತಂದರೆ ಅದನ್ನು ಅಪರಾಧವೆಂದು ಕರೆಯಬಹುದು. ಈ ರೀತಿಯ ಅಪರಾಧ ಇನ್ನೂ ಭಾರತದಲ್ಲಿ ಹೆಚ್ಚು ಪ್ರಧಾನವಾಗಿ ಕಂಡು ಬರದಿದ್ದರೂ, ಯೂರೋಪ್ ಮತ್ತು ಅಮೆರಿಕ ಗಳಲ್ಲಿ ವಿಷೇಶವಾದ ಪ್ರಾಮುಖ್ಯತೆಯನ್ನು ಪಡೆದುಕೊಂಡಿದೆ. ಇದರಿಂದ ಅಂತರ್ಜಾಲ ವ್ಯವಹಾರ ಮಾಡುವ ಸಾಫ್ಟ್‌ವೇರ್ ಕಂಪನಿಗಳು, ಹಾಗೂ ಬಿ.ಪಿ.ಓ. ಕಂಪನಿಗಳೂ ಹೆಚ್ಚಾಗಿ ಬಾಧಿಸಲ್ಪಡುತ್ತವೆ. ಮುಂಬರುವ ದಿನಗಳಲ್ಲಿ ಸೈಬರ್ ಕೆಫೆ ಗಳೂ ಇದರಿಂದ ಬಾಧಿತವಾಗುವ ಸಾಧ್ಯತೆಗಳಿವೆ.

ಅಧ್ಯಾಯ ೩ : ಕಾನೂನಿನ ವ್ಯಾಪ್ತಿ

ಹಿಂದಿನ ಅಧ್ಯಾಯದಲ್ಲಿ ನಾವು ಅಂತರ್ಜಾಲದಲ್ಲಿ ನಡೆಯಬಹುದಾದ ವಿವಿಧ ರೀತಿಯ ಅಪರಾಧಗಳನ್ನು ಸಮೀಕ್ಷಿಸಿದೆವು. ಈ ರೀತಿಯ ಅಪರಾಧಗಳು ನಡೆದಾಗ ಅಪರಾಧಿಯ ನೆಲೆಯನ್ನು ಗುರುತಿಸುವುದು ಹೇಗೆ ಮತ್ತು ಅವನು ಯಾವ ಕಾನೂನಿನ ವ್ಯಾಪ್ತಿಗೆ ಒಳಪಡುತ್ತಾನೆ ಎಂಬುದು ನಮ್ಮ ಮುಂದಿನ ಚಿಂತನೆ.

ಒಂದು ಅಪರಾಧ ನಡೆದಾಗ ಅದು ಎಲ್ಲಿ ನಡೆಯಿತು ಎಂಬುದು ಕಾನೂನಿನ ಪ್ರಕಾರ ಮುಖ್ಯ ಸಂಗತಿ . ಮೊದಲನೆಯದಾಗಿ ಅದು ಭಾರತದಲ್ಲಿ ನಡೆಯಿತೇ? ಅದಕ್ಕೆ ಭಾರತದ ಕಾನೂನಿನ ಚೌಕಟ್ಟಿನಲ್ಲಿ ಶಿಕ್ಷೆ ಇದೆಯೇ? ಎಂಬುದು ನಿರ್ಧಾರವಾಗಬೇಕು.

ಹಾಗೆಯೇ ಅಪರಾಧಿ ಭಾರತದಲ್ಲಿದ್ದಾನೆಯೇ? ಅವನು ಭಾರತದ ಪ್ರಜೆಯೇ? ಎಂಬುದೂ ನಿರ್ಧಾರವಾಗಬೇಕಾದ ಸಂಗತಿ.

ಮಾತಂಕಾ–೨೦೦೦ ಕಾನೂನಿನ ಪ್ರಕಾರ, ಯಾವುದೇ ಅಪರಾಧ ಭಾರತದ ಕಂಪ್ಯೂಟರ್ ಉಪಯೋಗಿಸಿ ನಡೆದಿದ್ದರೆ, ಅದು ಈ ಕಾನೂನಿನ ವ್ಯಾಪ್ತಿಗೆ ಬರುತ್ತದೆ. ಅಪರಾಧಿ ಭಾರತದ ಹೊರಗಿನ ನಿವಾಸಿಯಾಗಿದ್ದರೂ, ಅಥವಾ ವಿದೇಶೀ ಪ್ರಜೆಯಾಗಿದ್ದರೂ ಅವನು ಮಾತಂಕಾ–೨೦೦೦ ದ ಕಾನೂನಿನ ವ್ಯಾಪ್ತಿಗೆ ಬರುತ್ತಾನೆ.

ಆದರೆ ವಿದೇಶದಲ್ಲಿರುವ ಇತರ ದೇಶದ ಪ್ರಜೆಯೊಬ್ಬನ ಮೇಲೆ ನಮ್ಮ ಕಾನೂನಿನ ಪ್ರಕಾರ ಕ್ರಮ ಕೈಗೊಳ್ಳಬೇಕಾದರೆ ಅದಕ್ಕೆ ಎರಡು ದೇಶದ ನಡುವೆ ಒಂದು ಒಪ್ಪಂದ ಇದ್ದು ಅದರ ಪ್ರಕಾರ ಅಪರಾಧ ಎರಡೂ ದೇಶಗಳಲ್ಲೂ ಅಪರಾಧವೆಂದು ಪರಿಗಣಿಸಲ್ಪಟ್ಟಿರಬೇಕು.

ಸೈಬರ್ ಅಪರಾಧದಲ್ಲಿ ಅಪರಾಧಿಯ ಮೊದಲ ಗುರುತು ಅಪರಾಧ ಮಾಡಿದ ಕಂಪ್ಯೂಟರ್. ನಂತರ ಆ ಕಂಪ್ಯೂಟರ್ ನ ಮಾಲಿಕ ಅಥವಾ ಅದನ್ನು ಅಪರಾಧ ಸಂಭವಿಸಿದ ಸಮಯದಲ್ಲಿ ಆ ಕಂಪ್ಯೂಟರ್ ಉಪಯೋಗಿಸಿದವನ್ನು ''ಅಪರಾಧಿ'' ಎಂದು ಪರಿಗಣಿಸಬೇಕಾಗುತ್ತದೆ.

ನಾವು ಈಗಾಗಲೇ ತಿಳಿದಿರುವಂತೆ ಅಂತರ್ಜಾಲದಲ್ಲಿ ಜೋಡಣೆಯಾದ ಪ್ರತಿ ಕಂಪ್ಯೂಟರ್ ಗೂ ಒಂದು ನಿರ್ದಿಷ್ಟವಾದ ಐ.ಪಿ. ವಿಳಾಸ ಇರುತ್ತದೆ. ಈ ಐ.ಪಿ. ವಿಳಾಸ, ಆ ಕಂಪ್ಯೂಟರ್ ಅಂತರ್ಜಾಲದಲ್ಲಿ ಮಾಡುವ ಪ್ರತಿ ವ್ಯವಹಾರದಲ್ಲೂ ನಮೂದಿಸಲ್ಪಡುತ್ತದೆ. ಆದ್ದರಿಂದ ಯಾವುದೇ ಅಂತರ್ಜಾಲ ಅಪರಾಧ ನಡೆದಾಗಲೂ ಪೋಲೀಸರು ಮೊದಲು ಬೇಟೆಯಾಡುವುದು ಅಪರಾಧ ನಡೆದ ಕಂಪ್ಯೂಟರ್ ನ ಐ.ಪಿ. ವಿಳಾಸ. ಈ ಐ.ಪಿ. ವಿಳಾಸದಿಂದ ಆ ಕಂಪ್ಯೂಟರ್ ಯಾವ ಅಂತರ ಜಾಲ ಸೇವಾ ವ್ಯವಸ್ಥೆಯ ಒಳಗಿದೆ ಎಂಬುದನ್ನು ಒಡನೆಯೇ ತಿಳಿಯಬಹುದು.

ಇದರ ಪತ್ತೆಯಾದೊಡನೆ ಅದು ಯಾವ ಸೇವಾದಾರ (ಐ.ಎಸ್.ಪಿ) ನಿಗೆ ಸೇರಿದ್ದೆಂದು ನಿಗದಿಪಡಿಸಿ ಆ ಸೇವಾದಾರನ ಕಂಪ್ಯೂಟರ್ ಮೂಲಕ ಐ.ಪಿ. ವಿಳಾಸದ ನ ಮಾಲಿಕರನ್ನು ಹುಡುಕುವುದು ಸುಲಭದ ಕೆಲಸ. ಸೇವಾದಾರನ ದಾಖಲೆಯಲ್ಲಿ ಐ. ಪಿ ವಿಳಾಸ ಉಪಯೋಗಿಸಿದ ವ್ಯಕ್ತಿಯ ಪ್ರವೇಶ ಗುರುತು ಮತ್ತು ಅವನು ಉಪಯೋಗಿಸಿದ ದೂರವಾಣಿ ಸಂಖ್ಯೆ ತಿಳಿದುಬರುತ್ತದೆ.

ಕೆಲವು ಬಾರಿ ಈ ಐ.ಪಿ. ವಿಳಾಸ ಯಾವುದಾದರೂ ಸೈಬರ್ ಕೆಫೆ ಅಥವಾ ಕಂಪನಿಗೆ ಸೇರಿದ್ದಾಗಿರಬಹುದು. ಆಗ ಅಪರಾಧದ ಹೊಣೆಗಾರಿಕೆ ಆ ಸೈಬರ್ ಕೆಫೆ ಅಥವಾ ಕಂಪನಿಯಮೇಲೆ ಬೀಳುತ್ತದೆ. ಅಲ್ಲಿಯ ಅಧಿಕಾರಿಗಳು ತಮ್ಮದೇ ಆದ ದಾಖಲೆಗಳಿಂದ ಸೈಬರ್ ಕೆಫೆ ಅಥವಾ ಕಂಪನಿಯ ಯಾವ ಕಂಪ್ಯೂಟರ್ ನಿಂದ ಅಪರಾಧ ನಡೆದಿರಬಹುದು ಮತ್ತು ಅದನ್ನು ಮಾಡಿರಬಹುದಾದ ವ್ಯಕ್ತಿ ಯಾರಿರಬಹುದು ಎಂಬ ವಿಚಾರದ ಬಗೆ ಮಾಹಿತಿ ಒದಗಿಸಲು ಸಾಧ್ಯವಾದರೆ ಕಂಪನಿ

ಅಥವಾ ಸೈಬರ್ ಕೆಫೆ ಅಥವಾ ಅದರ ಅಧಿಕಾರಿಗಳ ವೈಯುಕ್ತಿಕ ಹೊಣೆಗಾರಿಕೆಯಿಂದ ಮುಕ್ತರಾಗಬಹುದು.

ಕೆಲವು ಬಾರಿ ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳು ನಡೆದಾಗ ಅದರ ನ್ಯಾಯಾಂಗ ವ್ಯಾಪ್ತಿಯನ್ನು ನಿರ್ಧರಿಸುವುದು ಜಟಿಲ ಸಮಸ್ಯೆಯಾಗುತ್ತದೆ. ಆದ್ದರಿಂದ ಅಪರಾಧ ಯಾವ ದೇಶದ ಕಾನೂನಿನ ವ್ಯಾಪ್ತಿಗೆ ಒಳಪಡುತ್ತದೆ? ಅಪರಾಧಿ ಬೇರೆ ದೇಶದಲ್ಲಿದ್ದರೆ ಅವನನ್ನು ಬಂಧಿಸಿ ಶಿಕ್ಷೆಗೆ ಒಳಪಡಿಸಬಹುದೇ? ಎಂಬ ಸಂದೇಹ ಬರುತ್ತದೆ.

ಏಕೆಂದರೆ ಅಂತರ್ಜಾಲ ಒಂದು ತ್ರಿಶಂಕು ಪ್ರದೇಶವಿದ್ದಂತೆ. ಅದು ಇಲ್ಲೂ ಇಲ್ಲ ಅಲ್ಲೂ ಇಲ್ಲ ಎಂಬಂತಹ ಪ್ರದೇಶ. ಉದಾಹರಣೆಗೆ ಅಮೆರಿಕಾದಲ್ಲಿನ ಕಂಪ್ಯೂಟರ್ ಮುಂದೆ ಕುಳಿತ ಒಬ್ಬ ವ್ಯಕ್ತಿ, ಆಸ್ಟ್ರೇಲಿಯಾ ದೇಶದ ವೆಬ್ ಸೈಟ್ ಒಂದರಿಂದ ಭಾರತದಲ್ಲಿರುವ ವ್ಯಕ್ತಿಗೆ ಯಾಹೂ ಇ–ಮೈಲ್ ವಿಳಾಸದ ಮೂಲಕ ಮೋಸದ ಸಮಾಚಾರವನ್ನು ಕಳುಹಿಸಬಹುದು. ಅದನ್ನು ಭಾರತದಲ್ಲಿರುವ ವ್ಯಕ್ತಿ ಅಮೆರಿಕಾದಲ್ಲಿರುವ ಯಾಹೂ ಸರ್ವರ್ ಸಂಪರ್ಕದಿಂದ ಪಡೆಯಬಹುದು. ಈ ಸಂದರ್ಭದಲ್ಲಿ ಅಪರಾಧ ಅಮೆರಿಕಾ ಸರ್ವರ್ ನಲ್ಲಿ ನಡೆಯಿತೇ? ಅಥವಾ ಆಸ್ಟ್ರೇಲಿಯಾದಲ್ಲಿ ನಡೆಯಿತೇ, ಅಥವಾ ಭಾರತದಲ್ಲಿ ನಡೆಯಿತೇ ಎಂಬುದು ವಿವಾದಾಸ್ಪದ ವಿಷಯ.

ಈಗಿರುವ ಕಾನೂನಿನ ಪ್ರಕಾರ, ಯಾವುದೇ ಅಪರಾಧದ ಪರಿಣಾಮ ಭಾರತದಲ್ಲಿ ಗ್ರಹಿಸಲ್ಪಟ್ಟಿದ್ದರೆ ಅಪರಾಧ ಇಲ್ಲಿ ನಡೆಯಿತೆಂದು ತಿಳಿಯಬಹುದು. ಇದಕ್ಕೆ ಮಾತಂಕಾ–೨೦೦೦ ಸಹ ಪುಷ್ಟಿ ಕೊಡುತ್ತದೆ. ಮಾತಂಕಾ ೨೦೦೦ ದ ಸೆಕ್ಷನ್ ೭೫ ರ ಪ್ರಕಾರ, ಅಪರಾಧದಲ್ಲಿ ಭಾರತದಲ್ಲಿರುವ ಯಾವುದೇ ಕಂಪ್ಯೂಟರ್ ಯಾವುದೇ ರೀತಿಯಲ್ಲಿ ಭಾಗಿಯಾಗಿದ್ದರೆ, ಆ ಅಪರಾಧ ಮಾತಂಕಾ ೨೦೦೦ ದ ವ್ಯಾಪ್ತಿಗೆ

ಒಳಪಡುತ್ತದೆ. ಅಲ್ಲದೆ ಅಪರಾಧಿ ವಿದೇಶೀ ಪ್ರಜೆಯಾಗಿದ್ದರೂ ಅಥವಾ ಭಾರತದ ಹೊರಗಿನ ನಿವಾಸಿಯಾಗಿದ್ದರೂ ಅವನು ಇಲ್ಲಿನ ಕಾನೂನಿಗೆ ಒಳಪಡುತ್ತಾನೆ.

ಹಾಗೆಯೇ ಮಾತಂಕಾ–೨೦೦೦ ದ ಪ್ರಕಾರ ಅಂತರ್ಜಾಲದಲ್ಲಿ ಇ–ಮೈಲ್ ಮೂಲಕ ಮಾಹಿತಿ ವಿನಿಮಯ ನಡೆದಾಗ ಇ–ಮೈಲ್ ಮಾಲಿಕ ವಾಸವಾಗಿರುವ ಸ್ಥಳವನ್ನು ಮಾಹಿತಿ ಹೊರಡುವ ಅಥವಾ ತಲುಪುವ ಸ್ಥಳವೆಂದು ತಿಳಿಯಲಾಗುತ್ತದೆ. ಉದಾಹರಣೆಗೆ ಬೆಂಗಳೂರಿನ ನಿವಾಸಿಯೊಬ್ಬ ತಾನು ಪ್ರವಾಸದಲ್ಲಿರುವಾಗ ಸಿಂಗಪೂರಿನಿಂದ ಇ–ಮೈಲ್ ಕಳುಹಿಸಿದರೆ ಅದು ಒಪ್ಪಂದಗಳ ಕಾನೂನಿನ ಚೌಕಟ್ಟಿನಲ್ಲಿ ಬೆಂಗಳೂರಿನಿಂದ (ಹಾಲಿ ವಾಸ ಸ್ಥಳ) ಕಳುಹಿಸಿದಂತೆ ಪರಿಗಣಿಸಲ್ಪಡುತ್ತದೆ.

ಇದೇ ನೀತಿಯನ್ನು ಪ್ರಯೋಗಿಸಿ ಯಾವುದೇ ಅಪರಾಧಕ್ಕೆ ಮಾತಂಕಾ–೨೦೦೦ ದ ಪ್ರಕಾರ ಕಾನೂನಿನ ವಾಪ್ತಿಯನ್ನು ನಿರ್ಧರಿಸಲು ಸಾಧ್ಯವಿದೆ.

ವಿದೇಶಗಳಲ್ಲಿ ಕೂಡ ಇದೇ ರೀತಿಯ ಕಾನೂನು ಜಾರಿಯಲ್ಲಿದ್ದು, ಅಪರಾಧದ ಪರಿಣಾಮ ಯಾವ ದೇಶದಲ್ಲಿ ಕಂಡು ಬರುತ್ತದೋ, ಯಾವ ದೇಶದ ಪ್ರಜೆಯ ಹಕ್ಕು ಭಾಧಿಸಲ್ಪಡುತ್ತದೋ, ಅಲ್ಲಿಯ ನ್ಯಾಯಾಲಯ ಮತ್ತು ಕಾನೂನಿನ ವ್ಯಾಪ್ತಿ ಆ ಅಪರಾಧಕ್ಕೆ ಇರುತ್ತದೆ. ಇದರಂತೆ ಮೈಸೂರಿನ ನಿವಾಸಿಯೊಬ್ಬ ಮಲೇಶಿಯ ಕಾನೂನಿನ ಪ್ರಕಾರ ಅಪರಾಧಿಯಾಗಬಹುದು. ರಷಿಯಾ ನಿವಾಸಿ ಅಮೆರಿಕಾ ಕಾನೂನಿನ ಪ್ರಕಾರ ಅಪರಾಧಿಯಾಗಬಹುದು. ಹಾಗೆ ನಡೆದಾಗ ಅಪರಾಧಿಯನ್ನು ಅಂತರ ರಾಷ್ಟ್ರೀಯ ಒಪ್ಪಂದಗಳ ಮೇರೆಗೆ ಶಿಕ್ಷೆಗೆ ಗುರಿಪಡಿಸಿಸುವ ಸಾಧ್ಯತೆ ಇದೆ ಎಂಬುದು ಗಮನದಲ್ಲಿಡಬೇಕಾದ ವಿಷಯ.

ಅಧ್ಯಾಯ ೪ : ಸೈಬರ್ ಸಾಕ್ಷ್ಯ

ನಾವು ಈಗಾಗಲೇ ಚರ್ಚಿಸಿದಂತೆ ಅಂತರ್ಜಾಲದಲ್ಲಿ ನಾವು ಅನೇಕ ಬಗೆಯ ಅಪರಾಧಗಳನ್ನು ಕಾಣುತ್ತೇವೆ. ಇದರಲ್ಲಿ ಕೆಲವು ನಮ್ಮನ್ನು ವೈಯುಕ್ತಿಕವಾಗಿ ಬಾಧಿಸಬಹುದು. ಇನ್ನು ಕೆಲವು ಬಾರಿ ನಾವು ಕೆಲಸ ಮಾಡುವ ಸಂಸ್ಥೆಯನ್ನು ಬಾಧಿಸಬಹುದು. ಅಥವಾ ನಾವು ಅಪರಾಧವನ್ನು ತನಿಖೆ ಮಾಡುವ ಅಧಿಕಾರಿಗಳಾಗಿರಬಹುದು. ಈ ಸಂದರ್ಭಗಳಲ್ಲಿ ನಾವು ಗಮನವಿಡಬೇಕಾದ ಅಂಶಗಳನ್ನು ಈಗ ನಾವು ಚರ್ಚಿಸೋಣ.

ಅಪರಾಧವೋ ಅಥವಾ ಅಪಘಾತವೋ:

ಅಂತರ್ಜಾಲದ ಅಪರಾಧಗಳನ್ನು ಸಮೀಕ್ಷಿಸುವಾಗ ನಾವು ಗಮನದಲ್ಲಿಡಬೇಕಾದ ಮುಖ್ಯ ಅಂಶವೇನೆಂದರೆ ಕೆಲವುಬಾರಿ ಅಪರಾಧದಂತೆ ಕಾಣುವ ಸಂಗತಿಗಳು ಬರಿಯ ಅಪಘಾತವಾಗಿರುವುದು.

ಯಾವುದಾದರೊಂದು ಅಪರಾಧ ಅದಕ್ಕೆ ಕಾರಣವಾಗಿರುವವರ ಅರಿವಿಗೆ ಬರದೆ ಅವರ ಉದ್ದೇಶವಿಲ್ಲದೆ ನಡೆದಿದ್ದರೆ ಅದನ್ನು ಅಪಘಾತವೆಂದು ಕರೆಯಬಹುದು. ಉದ್ದೇಶಪೂರ್ವಕವಾಗಿಯೋ ಅಥವಾ ಬೇಜವಾಬ್ದಾರಿತನದಿಂದಲೋ ನಡೆದಿದ್ದರೆ ಅದನ್ನು ಅಪರಾಧವೆಂದು ಪರಿಗಣಿಸಬಹುದು.

ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳಾದ ವೈರಸ್ ಪ್ರಸರಣ ಅಥವಾ ಸೈಬರ್ ಮುತ್ತಿಗೆ ಪ್ರಕರಣಗಳಲ್ಲಿ ನಿರಪರಾಧಿಗಳು ಸಿಕ್ಕಿಕೊಳ್ಳುವ ಅವಕಾಶ ಹೆಚ್ಚು. ಹಾಗೆಯೇ ಮತ್ತೊಬ್ಬರ ಹೆಸರಿನಲ್ಲಿ ಇ–ಮೈಲ್ ಅಥವಾ ಎಸ್.ಎಮ್.ಎಸ್ ಕಳುಹಿಸಿ ಅಥವಾ ಹ್ಯಾಕಿಂಗ್ ಮೂಲಕ ಮತ್ತೊಬ್ಬರ ಗಣಕ ಯಂತ್ರದೊಳಗೆ ನುಗ್ಗಿ ಅಪರಾಧ ಮಾಡಿದ ಪ್ರಕರಣಗಳಲ್ಲಿ ಕೂಡ ನಿರಪರಾಧಿಗಳು ಅಪರಾಧದ ಆರೋಪಿಗಳಾಗಬಹುದು.

ಅಂತೆಯೇ ಅಪರಾಧಗಳು ಆಫೀಸಿನ ಗಣಕ ಯಂತ್ರದಲ್ಲೋ ಅಥವಾ ಸೈಬರ್ ಕೆಫೆ ಮೂಲಕವೋ ನಡೆದರೆ ಅಲ್ಲಿನ ಅಧಿಕಾರಿಗಳು ಅಥವಾ ಮಾಲಿಕರು ಅಪರಾಧದ ಹೊಣೆ ಭರಿಸಬೇಕಾದ ಸಂಧರ್ಭ ಒದಗಿಬರಬಹುದು.

ಅನೇಕ ಪ್ರಸಂಗಗಳಲ್ಲಿ ಒಬ್ಬರ ಮೇಲಿನ ದ್ವೇಷಕ್ಕೋಸ್ಕರ ಸುಳ್ಳು ಮೊಕದ್ದಮೆ ಅಥವಾ ಸುಳ್ಳು ದೂರುಗಳನ್ನು ದಾಖಲು ಮಾಡಿ ನಿರಪರಾಧಿಗಳ ಶೋಷಣೆ ಮಾಡಿರುವುದೂ ಈಗಾಗಲೇ ಬೆಳಕಿಗೆ ಬಂದಿರುವ ವಿಷಯ.

ಸೈಬರ್ ಅಪರಾಧವೊಂದು ನಮ್ಮ ಗಮನಕ್ಕೆ ತರಪಟ್ಟಾಗ ಮೇಲೆ ತಿಳಿಸಿದಂತೆ ಅದು ಅಪಘಾತ, ನಿರ್ಲಕ್ಷ ಅಥವಾ ಶೋಷಣೆಯಾಗಿರುವ ಸಾಧ್ಯತೆಗಳನ್ನು ನೆನಪಿನಲ್ಲಿಟ್ಟುಕೊಂಡು ನಾವು ಮುಂದುವರೆಯಬೇಕಾದುದು ಬಹಳ ಅಗತ್ಯ.

ಉದಾಹರಣೆಗೆ ನಿಮಗೊಂದು ವೈರಸ್ ಇರುವ ಇ–ಮೈಲ್ ಒಂದು ಬಂತೆನ್ನೋಣ. ತಕ್ಷಣ ಇದು ಯಾರೋ ನಮ್ಮ ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿರುವ ಮಾಹಿತಿಯನ್ನು ನಷ್ಟಗೊಳಿಸಲು ಮಾಡಿರುವ ಪ್ರಯತ್ನ ಎಂದು ನಿರ್ಧರಿಸಿ ಅದನ್ನು ಕಳುಹಿಸಿದವರ ಬಗ್ಗೆ ಪೋಲೀಸರಿಗೆ ದೂರು ಕೊಡುವುದು ಬೇಡ.

ಏಕೆಂದರೆ ಅನೇಕ ಬಾರಿ ವೈರಸ್ ಗಳು ತಾವೇ ಇ–ಮೈಲ್ ಮೂಲಕ ಹರಡಿಕೊಳ್ಳುತ್ತಿರುತ್ತವೆ. ಈ ಸಮಯದಲ್ಲಿ ಅದು ತಾನು ಹೊರಬರುವ ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿನ ಇ–ಮೈಲ್ ವಿಳಾಸವನ್ನು ಹೊತ್ತು ಬರಬಹುದು. ಅಂತಹ ಸಂದರ್ಭಗಳನ್ನು ನಾವು ಅಪರಾಧ ಎಂದು ಕರೆಯುವುದಕ್ಕಿಂತ ನಮ್ಮಂತಹ ಇನ್ನೊಬ್ಬ ಕಂಪ್ಯೂಟರ್ ಒಡೆಯನ ನಿರ್ಲಕ್ಷತನ ನಡೆವಳಿಕೆಯಿಂದುಂಟಾದ ಅಪಘಾತವೆಂದು ಪರಿಗಣಿಸಬಹುದು.

ಕೆಲವು ಬಾರಿ ವೈರಸ್ ಗಳು ಯಾರದೋ ಹೆಸರಿನಲ್ಲಿ ಅವರ ಯಾವುದೇ ನಿರ್ಲಕ್ಷತೆ ಇಲ್ಲದೆಯೇ ಪ್ರಸರಣವಾಗಬಹುದು. ಇಂತಹ ಪ್ರಕರಣವನ್ನು ನಾವು ಅಪರಾಧವೆಂದು ಪರಿಗಣಿಸುವುದು ತಪ್ಪಾಗುತ್ತದೆ.

ಈ ರೀತಿಯ ವಿವೇಚನೆ ಎಲ್ಲಾ ಸೈಬರ್ ಅಪರಾಧ ಪ್ರಕರಣಗಳಲ್ಲೂ ಇರಬೇಕಾದುದು ಅತ್ಯಗತ್ಯ.

ಅಪರಾಧಕ್ಕೆ ಸಾಕ್ಷಿ:

ಯಾವುದೇ ಅಪರಾಧ ನಡೆದಾಗ ಅದು ನಡೆದಿದೆಯೆಂಬ ಬಗ್ಗೆಗಿನ ಸಾಕ್ಷಿ ಬಹು ಮುಖ್ಯ. ಉದಾಹರಣೆಗೆ ಒಬ್ಬ ಪೋಲೀಸ್ ಠಾಣೆಗೆ ಬಂದು ರಸ್ತೆಯಲ್ಲಿ ಒಬ್ಬ ವ್ಯಕ್ತಿ ಕೊಲೆಯಾಗಿ ಅವನ ಹೆಣ ಬಿದ್ದಿದೆ ಎಂದು ತಿಳಿಸುತ್ತಾನೆ ಎಂದುಕೊಳ್ಳೋಣ. ಆದರೆ ಪೋಲೀಸರು ಸ್ಥಳಕ್ಕೆ ಬಂದಾಗ ಮೃತ ದೇಹ ದೊರೆಯದೆ ಹೋದರೆ ಪೋಲೀಸರು ದೂರನ್ನು ದಾಖಲಿಸಿಕೊಂಡು ಮುಂದುವರೆಯುವುದು ಕಷ್ಟವಾಗುತ್ತದೆ. ಅಪರಾಧ ನಡೆದಿದೆಯೇ ಇಲ್ಲವೇ ಎಂಬುದೇ ವಿವಾದಾಸ್ಪದವಾಗುತ್ತದೆ.

ಇದೇ ರೀತಿ ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳಲ್ಲಿ ನಡೆಯುವ ಸಾಧ್ಯತೆ ಬಹಳಷ್ಟು ಇದೆ.

ಉದಾಹರಣೆಗೆ ಒಬ್ಬ ವ್ಯಕ್ತಿ ತನ್ನ ಬಗ್ಗೆ ವೆಬ್ ಸೈಟ್ ಒಂದರಲ್ಲಿ ತಪ್ಪು ಮಾಹಿತಿಯನ್ನು ಪ್ರಕಟಮಾಡಿ ಮಾನನಷ್ಟ ವಾಗಿದೆಯೆಂದು ದೂರು ಕೊಡುತ್ತಾನೆಂದುಕೊಳ್ಳೋಣ. ಆಗ ಅವನು ಅದರ ಬಗ್ಗೆ ಸಾಕ್ಷಿ ಕೊಡಬೇಕಾಗುತ್ತದೆ. ಅವನು ತಕ್ಷಣ ಸಾಕ್ಷಿಯನ್ನು ಹೊಂದಿಸಿಕೊಳ್ಳದಿದ್ದರೆ ತನಿಖೆ ನಡೆಯುವ ಮುನ್ನ ಆ ತಪ್ಪು ಮಾಹಿತಿಯನ್ನು ವೆಬ್ ಸೈಟ್ ಒಡೆಯ ತೆಗೆದು ಹಾಕಿಬಿಡಬಹುದು. ಅಥವಾ ತನಿಖೆಯಲ್ಲಿ ಕಂಡು ಬಂದರೂ ನ್ಯಾಯಾಲಯದಲ್ಲಿ ಪ್ರತಿವಾದಿ ಸಾಕ್ಷ್ಯವನ್ನು ಸುಳ್ಳು ಎಂದು ಪ್ರತಿಪಾದಿಸಿದಾಗ ನ್ಯಾಯಾಲಯಕ್ಕೆ ಸಾಕ್ಷ್ಯ ಲಭ್ಯವಾಗದೆ ಹೋಗಬಹುದು.

ಇಂತಹ ಪ್ರಸಂಗಕ್ಕೆ ನನ್ನ ಅನುಭವಕ್ಕೆ ಬಂದ ಒಂದು ಉತ್ತಮ ಉದಾಹರಣೆ ಒಂದು ಹೆಸರಾಂತ ಪತ್ರಿಕೆ ತನ್ನ ವೆಬ್ ಸೈಟ್ ಜಾಹೀರಾತಿನಲ್ಲಿ ಮೋಸ ಮಾಡಲು ಪ್ರಯತ್ನಿಸಿದುದು. ಈ ಪ್ರಸಂಗದಲ್ಲಿ ಚೆನ್ನೈ ನ ಒಂದು ಕಂಪನಿ ಈ ಪತ್ರಿಕೆಯ ವೆಬ್ ಸೈಟ್ ನಲ್ಲಿ ತಿಂಗಳು ಪೂರಾ ಪ್ರಕಟವಾಗಬೇಕೆಂದು ಜಾಹೀರಾತನ್ನು ಕೊಟ್ಟಿತ್ತು. ಆದರೆ ಆ ಪತ್ರಿಕೆ ರಾತ್ರಿ ಹತ್ತು ಘಂಟೆಯ ನಂತರ ಜಾಹೀರಾತನ್ನು ತೆಗೆದು ಹಾಕಿ ಬೇರೊಂದು ಜಾಹೀರಾತನ್ನು ಅದೇ ಜಾಗದಲ್ಲಿ ಪ್ರಕಟಮಾಡುತ್ತಿತ್ತು. ಮತ್ತೆ ಬೆಳಗಿನ ಹೊತ್ತಿಗೆ ಕಂಪನಿಯ ಜಾಹೀರಾತು ಇರುತ್ತಿತ್ತು. ಕಂಪನಿ ಅಧಿಕಾರಿಗಳು ಬೆಳಗಿನ ಹೊತ್ತು ವೆಬ್ ಸೈಟ್ ಗೆ ಹೋದಾಗಲೆಲ್ಲಾ ಜಾಹಿರಾತು ಇರುತ್ತಿದ್ದುದರಿಂದ ಈ ಮೋಸ ಬೆಳಕಿಗೆ ಬರಬೇಕಾದರೆ ಅನೇಕ ದಿನಗಳೇ ಬೇಕಾಯಿತು. ಈ ಸಂದರ್ಭದಲ್ಲಿ ನಿಗದಿತ ಸಮಯದಲ್ಲಿ ಕಂಪನಿ ಜಾಹಿರಾತು ಇರಬೇಕಾದ ಸಮಯದಲ್ಲಿ ಬೇರೆ ಜಾಹಿರಾತು ಇತ್ತು ಎಂದು ದೂರು ಕೊಡುವವರು ಆಧಾರಪೂರ್ವವಾಗಿ ನಿರೂಪಿಸುವುದು ಒಂದು ಸಮಸ್ಯೆಯಾಗುತ್ತದೆ.

ಇನ್ನೊಂದು ಇದೇ ರೀತಿಯ ಪ್ರಕರಣದಲ್ಲಿ ಚೆನ್ನೈ ನ ಪ್ರಮುಖ ತಮಿಳು ಪತ್ರಿಕೆಯ ವೆಬ್ ಸೈಟ್ ನಲ್ಲಿ ಜಾಹಿರಾತು ಒಂದನ್ನು ತೆಗೆದು ಹಾಕಿ ಕೆಲವು ಘಂಟೆಗಳ ಕಾಲ ಸರ್ಕಾರಿ ವಿರೋಧಿ ಘೋಷಣೆಯನ್ನು ಪತ್ರಿಕೆಯ ಉದ್ಯೋಗಿಗಳಲ್ಲೊಬ್ಬ ಪ್ರಕಟಿಸಿದ್ದ. ಪತ್ರಿಕೆಯ ಅಧಿಕಾರಿ ವಿಷಯ ತಿಳಿದೊಡನೆ ಆ ಘೋಷಣೆಗಳನ್ನು ತೆಗೆದು ಮುಂಚಿನ ಜಾಹಿರಾತನ್ನು ಹಾಕಿ ತಪ್ಪನ್ನು ಸರಿಪಡಿಸಿದ. ಅವನು ಹಾಗೆ ಮಾಡದಿದ್ದರೆ ಪ್ರತಿ ನಿಮಿಷ ವೆಬ್ ಸೈಟ್ ಗೆ ಬರುವ ಹಲವಾರು ಜನರು ಆ ಘೋಷಣೆಗಳನ್ನು ಕಾಣುವ ಅವಕಾಶವಿತ್ತು.

ಆದರೆ ಈ ಪ್ರಕರಣದಲ್ಲಿ ದೂರು ದಾಖಲು ಮಾಡಬೇಕಾದರೆ ಕಂಪನಿಗೆ ಕೆಲವು ಅಡಚಣೆಗಳು ಕಂಡುಬರುತ್ತವೆ. ಏಕೆಂದರೆ ದೂರು ಕೊಡುವ ಸಮಯ ದಲ್ಲಿ ಅಪರಾಧದ ಸುಳಿವು ಮರೆಯಾಗಿರುತ್ತದೆ. ಇಂತಹ ದೂರನ್ನು ನಿರೂಪಿಸಬೇಕಾದರೆ ಆ

ಘೋಷಣೆಗಳನ್ನು ವೆಬ್ ಸೈಟ್ ನಲ್ಲಿ ನೋಡಿದ ಗ್ರಾಹಕರಾರಾದರೂ ವೈಯುಕ್ತಿಕವಾಗಿ ಸಾಕ್ಷಿ ಹೇಳಬೇಕಾಗುತ್ತದೆ. ಆ ಸಾಕ್ಷಿ ನ್ಯಾಯಲಯಕ್ಕೆ ಬಂದಾಗ ಪ್ರತಿವಾದಿ ವಕೀಲರು ಈ ಸಾಕ್ಷಿಗೂ, ದೂರು ನೀಡಿದವನಿಗೂ ಅನ್ಯೆತಿಕವಾದ ಒಡಂಬಡಿಕೆ ಇದೆಯೆಂದೂ ಆದ್ದರಿಂದ ಅವನು ಸುಳ್ಳು ಸಾಕ್ಷಿ ನೀಡುತ್ತಿದ್ದಾನೆಂದೂ ಹೇಳಿದರೆ ಸಾಕ್ಷಿಯನ್ನು ನಿರೂಪಿಸುವುದು ಕಷ್ಟವಾಗುತ್ತದೆ.

ನನ್ನ ಗಮನಕ್ಕೆ ಬಂದ ಮತ್ತೊಂದು ಶೋಷಣೆ ಪ್ರಸಂಗದಲ್ಲಿ ಒಬ್ಬ ಹುಡುಗಿ ತನ್ನ ಇ–ಮೈಲ್ ಪೆಟ್ಟಿಗೆಯಿಂದ ತನ್ನ ತಂದೆಯ ಇ–ಮೈಲ್ ಪೆಟ್ಟಿಗೆಗೆ ಕಳುಹಿಸಲ್ಪಟ್ಟಿದೆಯೆನ್ನಲಾದ ಇ–ಮೈಲ್ ಒಂದನ್ನು ಆಧಾರವಾಗಿಟ್ಟುಕೊಂಡು ತನ್ನ ಸಹೋದ್ಯೋಗಿಯ ಮೇಲೆ ಸುಳ್ಳು ದೂರೊಂದನ್ನು ಸಲ್ಲಿಸಿದ್ದಳು. ಆದರೆ ದೂರು ಕೊಡುವವನೊಬ್ಬ ತನ್ನದೇ ಅಧೀನದಲ್ಲಿದ್ದ ಗಣಕ ಯಂತ್ರದಿಂದ ತೆಗೆದ ಮಾಹಿತಿಯನ್ನು ಸಾಕ್ಷಿಯೆಂದು ಪರಿಗಣಿಸಿ ಅದರ ಆಧಾರದಿಂದ ಹೊರಗಿನವನೊಬ್ಬನನ್ನು ಅಪರಾಧಿಯೆಂದು ಪರಿಗಣಿಸುವುದು ಅಪಾಯಕಾರಿ. ಅಂತಹ ಸಾಕ್ಷಿ ದಾಖಲೆಗಳನ್ನು ನ್ಯಾಯಾಲಯ ತಿರಸ್ಕರಿಸುವ ಸಾಧ್ಯತೆಯೇ ಹೆಚ್ಚು.

ಈ ಸಮಸ್ಯೆಗಳನ್ನು ನೆನಪಿನಲ್ಲಿಟ್ಟುಕೊಂಡು ದೂರು ನೀಡಬೇಕಾದ ಯಾರೇ ಆದರೂ ದೂರು ನೀಡುವ ಮೊದಲೇ ಸರಿಯಾದ ಸಾಕ್ಷಿ ದಾಖಲೆಯನ್ನು ತೆಗೆದುಕೊಳ್ಳಬೇಕಾದುದು ಮುಖ್ಯ.

ಇಂತಹ ಪ್ರಸಂಗಗಳಲ್ಲಿ ಉಪಯೋಗವಾಗುವುದಕ್ಕೆ ಅಂತರ್ಜಾಲದಲ್ಲೇ ಸಾಕ್ಷಿಯನ್ನು ದಾಖಲು ಮಾಡಿಕೊಂಡು ನ್ಯಾಯಾಲಕ್ಕೆ ಒಪ್ಪಿಗೆಯಾಗಬಹುದಾದ ರೀತಿಯಲ್ಲಿ ಪ್ರಮಾಣ ಪತ್ರವನ್ನು ನೀಡುವ ಸೇವೆ ,ಸೈಬರ್ ಎವಿಡೆನ್ಸ್ ಆರ್ಕೈವಲ್ ಸೆಂಟರ್ (www.ceac4india.com) ಎಂಬ ವೆಬ್ ಸೈಟ್ ಮೂಲಕ ಒದಗಿಬರುತ್ತಿದೆ. ಈ ಸೇವೆಯನ್ನು ಸಾಮಾನ್ಯ ಜನರಾಗಲೀ ಅಥವಾ ಪೋಲೀಸರಾಗಲೀ ಉಪಯೋಗಿಸಿಕೊಳ್ಳಬಹುದು.

ಇಲ್ಲದಿದ್ದರೆ ಪ್ರಕರಣ ಬೆಳಕಿಗೆ ಬಂದೊಡನೆ ಸೈಬರ್ ಸಾಕ್ಷಿ ನಿಪುಣರನ್ನು ಸಂಪರ್ಕಿಸುವುದು ಅಗತ್ಯ.

ಕೆಲವು ಸಂದರ್ಭಗಳಲ್ಲಿ ವಿಶೇಷ ಉಪಕರಣಗಳನ್ನೂ, ತಂತ್ರಾಂಶಗಳನ್ನೂ ಉಪಯೋಗಿಸಿ ಸಾಕ್ಷಿ ದಾಖಲೆಗಳನ್ನು ಹೊಂದಿಸಬೇಕಾಗಬಹುದು. ಇದೆಲ್ಲವನ್ನೂ ಹೆಚ್ಚು ಕಾಲ ಹರಣ ಮಾಡದೆ ಮಾಡುವುದು ಉತ್ತಮ.

ಅನೇಕ ಪ್ರಕರಣಗಳಲ್ಲಿ ಸಾಕ್ಷಿ ಬಲವಾಗಿಲ್ಲದೆ ಹೋದರೆ ಅಪರಾಧಿಗೆ ಶಿಕ್ಷೆಯಾಗದೆ, ದೂರು ಕೊಟ್ಟವರೇ ಸುಳ್ಳು ದೂರನ್ನು ದಾಖಲಿಸಿದ ಆರೋಪಕ್ಕೆ ಗುರಿಯಾಗಬೇಕಾಗುತ್ತದೆ.

ಕಂಪ್ಯೂಟರ್ ದಾಖಲೆಗಳನ್ನು ಸಾಕ್ಷಿಯಾಗಿ ಸ್ವೀಕರಿಸುವುದಕ್ಕೆ ಅನುಕೂಲವಾಗುವಂತೆ ಮಾತಂಕಾ-೨೦೦೦ ದೊಡನೆ, ಭಾರತೀಯ ಸಾಕ್ಷಿ ಕಾನೂನಿಗೆ ಅನೇಕ ಬದಲಾವಣೆಗಳನ್ನು ತರಲಾಗಿದೆ. ಇದರಂತೆ, ಇಂಡಿಯನ್ ಎವಿಡೆನ್ಸ್ ಆ್ಯಕ್ಟ್ ಸೆಕ್ಷನ್ ೬೫ ಬಿ ಪ್ರಕಾರ ಯಾವುದೇ ಗಣಕ ಯಂತ್ರದ ದಾಖಲೆಯನ್ನು, ಸರಿಯಾದ ಪ್ರಮಾಣಪತ್ರದೊಡನೆ ಮುದ್ರಿತ ರೂಪದಲ್ಲೂ ನ್ಯಾಯಾಲಯಕ್ಕೆ ಸಲ್ಲಿಸಬಹುದು.

ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳನ್ನು ನಿರೂಪಿಸಲು ಈ ಕಾನೂನಿನ ಅವಶ್ಯತೆಗಳನ್ನು ಅರಿತುಕೊಂಡು ಅದರಂತೆ ಸಾಕ್ಷಿ ದಾಖಲೆಗಳನ್ನು ನ್ಯಾಯಾಲಯಕ್ಕೆ ಸಲ್ಲಿಸುವುದು ಪೋಲೀಸರ ಕರ್ತವ್ಯ. ಈ ರೀತಿ ಸರಿಯಾದ ಸಾಕ್ಷಿಯನ್ನು ಒದಗಿಸಿ ಭಾರತದಲ್ಲಿಯೇ ಪ್ರಥಮವಾಗಿ ಮಾತಂಕಾ ೨೦೦೦ ದ ಸೆಕ್ಷನ್ ೬೭ ರ ಪ್ರಕಾರ ತೀರ್ಪನ್ನು ಪಡೆದ ಕೀರ್ತಿ ತಮಿಳು ನಾಡು ಪೋಲಿಸರಿಗೆ ಇದೇ ನವೆಂಬರ್ ೫, ೨೦೦೪ ನೇ ದಿನಾಂಕ ಒದಗಿಬಂತು. ಈ ಪ್ರಕರಣದಲ್ಲಿ ಚೆನ್ನೈ ನ ಮಹಿಳೆಯೊಬ್ಬಳ ಬಗ್ಗೆ ಅಶ್ಲೀಲ ಸಮಾಚಾರವನ್ನು ಅಂತರ್ಜಾಲದಲ್ಲಿ ಬಿತ್ತರ ಮಾಡಿದ ಪ್ರಯುಕ್ತ ಚೆನ್ನೈನ ನ್ಯಾಯಾಲಯ ಮುಂಬೈನ ಸುಹಾಸ್ ಕಟ್ಟಿ ಎಂಬ ಯುವಕನಿಗೆ ಮಾತಂಕಾ ೨೦೦೦ ದ

ಒಳಗೆ ೨ ವರ್ಷ ಮತ್ತು ಇತರ ಕಾನೂನಿನ ನಡುವೆ ೩ ವರ್ಷ ದಂಡನೆ ವಿಧಿಸಿ ತೀರ್ಪು ಕೊಟ್ಟಿತು. ಈ ಪ್ರಕರಣದಲ್ಲಿ ದೂರು ಕೊಟ್ಟ ೪ ದಿನದೊಳಗೆ ಅಪರಾಧಿಯನ್ನು ಕಂಡು ಹಿಡಿದು ವಶಕ್ಕೆ ತೆಗೆದುಕೊಂಡ ಪೋಲೀಸರು ಪ್ರಕರಣವನ್ನು ಕೇವಲ ೮ ತಿಂಗಳಲ್ಲಿ ಮುಗಿಸಿ ಅಂತರ್ಜಾಲ ಅಪರಾಧಿಗಳಿಗೆ ಎಚ್ಚರಿಕೆ ನೀಡುವುದರಲ್ಲಿ ಯಶಸ್ವಿಯಾಗಿದ್ದಾರೆ. ಈ ಪ್ರಸಂಗದಲ್ಲಿ ಸೈಬರ್ ಎವಿಡೆನ್ಸ್ ಆರ್ಕೈವಲ್ ಸೆಂಟರ್ ನ ಸಹಾಯವನ್ನು ಪೋಲೀಸರು ಯಶಸ್ವಿಯಾಗಿ ಉಪಯೋಗಿಸಿಕೊಂಡರೆಂಬುದು ಗಮನದಲ್ಲಿಡಬೇಕಾದ ಸಂಗತಿ.

ಇದೇ ರೀತಿ ಮುಂದೆಯೂ ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳ ಪ್ರಸಂಗಗಳಲ್ಲಿ ನಿಜವಾದ ಅಪರಾಧಿಗಳನ್ನು ಕಂಡು ಹಿಡಿದು ಅವರಿಗೆ ಶ್ರೀಘ್ರವಾಗಿ ಶಿಕ್ಷೆ ಒದಗಿಸಬೇಕಾದರೆ ಸೈಬರ್ ಸಾಕ್ಷಿಯನ್ನು ಸರಿಯಾಗಿ ಉಪಯೋಗಿಸಿಕೊಳ್ಳಬೇಕಾದುದು ಅಗತ್ಯ. ಇದರ ಬಗ್ಗೆ ಪರಿಣಿತಿಯನ್ನೂ, ಹಾಗೂ ಬೇಕಾದ ಉಪಕರಣಗಳನ್ನೂ ನಮ್ಮ ಪೋಲೀಸರು ಆದಷ್ಟು ಬೇಗ ಪಡೆದುಕೊಳ್ಳಬೇಕಾದುದೂ ಅಗತ್ಯ.

Cyber Evidence Archival Center

http://www.naavi.org

ಅಧ್ಯಾಯ ೫ : ಭಾರತದಲ್ಲಿನ ಸೈಬರ್ ಕಾನೂನು

ಇಂದು ಭಾರತದ ಸೈಬರ್ ಕಾನೂನಿನ ಮುಖ್ಯ ಅಂಗ ವೆಂದರೆ ಅಕ್ಟೋಬರ್ ೧೭, ೨೦೦೦ ರಿಂದ ಜಾರಿಗೊಂಡ ಇನ್ಫರ್ಮೇಶನ್ ಟೆಕ್ನಾಲಜಿ ಆಕ್ಟ್ ಅಥವಾ ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯಿದೆ ೨೦೦೦ (ಮಾತಂಕಾ ೨೦೦೦) ಮೂಲಕ. ಇದಕ್ಕೆ ಮುನ್ನವೇ ಕಾಪಿರೈಟ್ ಆಕ್ಟ್ ನಲ್ಲಿ ಆ ಕಾಯಿದೆಯನ್ನು ಕಂಪ್ಯೂಟರ್ ಕೆಲಸಗಳಿಗೆ ವಿಸ್ತರಿಸಲಾಗಿದ್ದರೂ, ಮೊತ್ತ ಮೊದಲ ಬಾರಿಗೆ ''ಗಣಕ ದಾಖಲೆ'' ಅಥವಾ ''ವಿದ್ಯುನ್ಮಾನ ದಾಖಲೆ'' (ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಡಾಕ್ಯುಮೆಂಟ್) ಎಂಬ ಪದದ ಪ್ರಯೋಗವಾದುದು ಮಾತಂಕಾ ೨೦೦೦ ಮೂಲಕ.

ಮಾತಂಕಾ ಕಾಯಿದೆ ಮೊದಲಬಾರಿಗೆ ಭಾರತದಲ್ಲಿ ಗಣಕ ದಾಖಲೆಗಳು ಕಾನೂನಿನ ಪ್ರಕಾರ ಬರವಣಿಗೆಯಲ್ಲಿ ಕೊಟ್ಟ ಪತ್ರಗಳಷ್ಟೇ ಊರ್ಜಿತವಾಗುತ್ತವೆಂದು ಘೋಷಿಸಿದೆ. ಸರ್ಕಾರಿ ವ್ಯವಹಾರಗಳಲ್ಲಿ ಗಣಕ ಪತ್ರಗಳ ಬಳಕೆಯ ಉಪಯೋಗಕ್ಕೆ ಅನುಮತಿ ಕೂಡ ಈ ಕಾಯಿದೆ ಮೂಲಕ ನೀಡಲಾಗಿದೆ. ಅಲ್ಲದೆ ಈ ಕಾಯಿದೆಯಲ್ಲಿ ಗಣಕ ದಾಖಲೆಗಳನ್ನು ಧೃಡೀಕರಿಸುವ (ಸಹಿ ಮಾಡುವ) ವಿಧಾನ, ಮತ್ತು ಒಪ್ಪಂದಗಳನ್ನು ಮಾಡಿಕೊಳ್ಳುವ ವಿಧಾನವನ್ನು ಪ್ರಸ್ತಾಪ ಮಾಡಲಾಗಿದೆ. ಇದಲ್ಲದೆ ಕೆಲವು ಸೈಬರ್ ಕ್ರೈಂ ಅಥವಾ ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳ ಬಗ್ಗೆಯೂ ಪ್ರಸ್ತಾಪಿಸಲಾಗಿದ್ದು ಅವುಗಳಿಗೆ ಕೊಡಬಹುದಾದ ಶಿಕ್ಷೆಗಳ ಬಗ್ಗೆ ಮತ್ತು ಅವುಗಳಿಗೆ ವಿಶೇಷ ನ್ಯಾಯಾಂಗ ವ್ಯವಸ್ಥೆಯ ಬಗ್ಗೆಯೂ ಪ್ರಸ್ತಾಪವಿದೆ. ಇದರೊಡನೆ ಕಂಪ್ಯೂಟರ್ ಜಾಲಗಳ ಒಡೆಯರು ತೆಗೆದುಕೊಳ್ಳಬೇಕಾದ ಜವಾಬ್ದಾರಿಗಳ ಬಗ್ಗೆಯೂ ಪ್ರಸ್ತಾಪವಿದೆ.

ಇವೆಲ್ಲದರ ಸಂಕ್ಷಿಪ್ತ ವಿವರಣೆ ಕೆಳಗೆ ನೀಡಲಾಗಿದೆ. (ಹೆಚ್ಚಿನ ವಿವರಗಳಿಗೆ ಓದುಗರು www.naavi.org ವೆಬ್ ಸೈಟ್ ನೋಡಬಹುದು.)

ಈಗ ಕೆಲವು ವರ್ಷಗಳಿಂದ ಕರ್ನಾಟಕ ಸರ್ಕಾರದಲ್ಲಿ ಗಣಕ ಯಂತ್ರಗಳ ಬಳಕೆ ನಡೆಯುತ್ತಿದೆ. ಈ ಇ–ಆಡಳಿತದ ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ಒಂದು ಮುಖ್ಯ ಸೇವೆ, ''ಭೂಮಿ'' ಹೆಸರಿನ ಭೂ ದಾಖಲೆಗಳ ದಾಖಲೀಕರಣ. ಈ ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ಜನ ಸಾಮಾನ್ಯರು, ಹಳ್ಳಿ ಹಳ್ಳಿಗಳಲ್ಲೂ ಬಳಸುವ ''ಪಹಣಿ'' ಪತ್ರದಂತಹ ದಾಖಲೆಗಳನ್ನು ಗಣಕ ಯಂತ್ರದ ಮೂಲಕ ನೀಡುವ ವ್ಯವಸ್ಥೆ ಮಾಡಲಾಗಿದೆ. ಇದಕ್ಕಾಗಿ ಬೇಕಾದ ಬದಲಾವಣೆಗಳನ್ನು ರೆವೆನ್ಯೂ ಆ್ಯಕ್ಟ್ ಗಳಲ್ಲಿ ಮಾಡಲಾಗಿದೆ. ಇದರಿಂದ ಸೈಬರ್ ಕಾನೂನಿನ ವ್ಯಾಪ್ತಿ ವಿಸ್ತಾರವಾಯಿತೆನ್ನಬಹುದು.

ಇತ್ತೀಚೆಗಷ್ಟೆ ಸರ್ಕಾರ ಕರ್ನಾಟಕ ದಲ್ಲಿರುವ ೫೦,೦೦೦ ಕ್ಕೂ ಹೆಚ್ಚು ಸೈಬರ್ ಕೆಫೆ ಗಳನ್ನು ನಿಯಂತ್ರಿಸಲು ಕಾನೂನನ್ನು ತಂದಿದೆ. ಇದರ ಮುಖ್ಯ ಅಂಶಗಳನ್ನು ಕೂಡ ಈ ಪುಸ್ತಕದಲ್ಲಿ ಪ್ರತ್ಯೇಕವಾಗಿ ವಿವರಿಸಲಾಗಿದೆ.

ಮಾತಂಕಾ ೨೦೦೦ ದ ಮುಖ್ಯಾಂಶಗಳು

(ವಿ.ಸೂ: ಈ ವಿಭಾಗದಲ್ಲಿ ಮತ್ತು ಪುಸ್ತಕದ ಇತರ ಕಡೆಗಳಲ್ಲಿ ಇನ್ಫರ್ಮೇಶನ್ ಟೆಕ್ನಾಲಜಿ ಆ್ಯಕ್ಟ್ ೨೦೦೦ ದ ವಿವಿಧ ಸೆಕ್ಷನ್ ಗಳ ಕನ್ನಡ ಅನುವಾದ ವನ್ನು ಜನ ಸಾಮಾನ್ಯರ ತಿಳುವಳಿಕೆಗಾಗಿ ಕೊಟ್ಟಿರುತ್ತದೆ. ಇದು ಅಧಿಕೃತ ಅಥವಾ ಸಂಪೂರ್ಣ ಅನುವಾದ ವಲ್ಲ. ಓದುಗರು ಅಧಿಕೃತ ವಿವರಗಳಿಗೆ ಆ್ಯಕ್ಟ ನ ಇಂಗ್ಲಿಷ್ ಆವೃತ್ತಿಯನ್ನು ಪರಿಶೀಲಿಸಬೇಕೆಂದು ಕೋರಲಾಗಿದೆ. ಇತ್ತೀಚಿನ ಆವೃತ್ತಿಯನ್ನು www.naavi.org ಯಲ್ಲಿ ಪಡೆಯಬಹುದು. ಕನ್ನಡ ಅನುವಾದದಿಂದ ಯಾರಿಗಾದರೂ ತಪ್ಪು ಅಭಿಪ್ರಾಯ ಮೂಡಿದಲ್ಲಿ ಹಾಗೂ ಅದರಿಂದ ಯಾವುದೇ ನಷ್ಟ ಸಂಭವಿಸಿದಲ್ಲಿ ಈ ಪುಸ್ತಕದ ಲೇಖಕರಾಗಲೀ, ಪ್ರಕಟನ ಸಂಸ್ಥೆಯಾಗಲೀ ಹೊಣೆಯಲ್ಲ ಎಂಬುದನ್ನು ಈ ಮೂಲಕ ತಿಳಿಯಪಡಿಸಲಾಗಿದೆ.)

ಕಾನೂನಿನ ಅನುಮೋದನೆ

ಮಾತಂಕಾ ೨೦೦೦ ಸೆಕ್ಷನ್ ೪ ರ ಪ್ರಕಾರ ಭಾರತದ ಯಾವುದೇ ಕಾನೂನಿನಲ್ಲಿ ಬರವಣಿಗೆಯ ಮೂಲಕ ಯಾವುದೇ ದಾಖಲೆಯನ್ನು ಸಲ್ಲಿಸಬೇಕೆಂದು ನಮೂದಿಸಲ್ಪಟ್ಟಿದ್ದರೆ ಆ ದಾಖಲೆಯನ್ನು ಗಣಕ ಪತ್ರದ ರೂಪದಲ್ಲಿ ಸಲ್ಲಿಸಬಹುದು.

ಆದರೆ ಸೆಕ್ಷನ್ ೧ ರ ಪ್ರಕಾರ ಕೆಲಕಂಡ ದಾಖಲೆಗಳಿಗೆ ಮಾತಂಕಾ ಅನ್ವಯಿಸುವುದಿಲ್ಲವಾದ್ದರಿಂದ ಅಂತಹ ದಾಖಲೆಗಳು ಮಾತಂಕಾ ಕಾಯಿದೆಯ ಹೊರಗೆ ಉಳಿಯುತ್ತದೆ. ಮಾತಂಕಾ ದ ಚೌಕಟ್ಟಿನ ಹೊರಗೆ ಇರುವ ವ್ಯವಹಾರಗಳಿಂದರೆ,

೧) ಪ್ರಾಮಿಸರಿ ನೋಟ್ ಮತ್ತು ಹುಂಡಿ ಪತ್ರಗಳು
೨) ಪವರ್ ಆಫ್ ಅಟ್ಟಾರ್ನಿ ಪತ್ರ
೩) ಟ್ರಸ್ಟ್ ಪತ್ರ

೪) ಉಯಿಲು

೫) ಸ್ಥಿರ ಆಸ್ಥಿ ಕ್ರಯ ಪತ್ರ ಅಥವಾ ಪರಭಾರೆ ಪತ್ರ

ಮಾತಂಕಾ ಜಾರಿಗೆ ಬಂದಾಗ ಬ್ಯಾಂಕ್ ಚೆಕ್ ಕೂಡಾ ಈ ಕಾಯಿದೆಗೆ ಹೊರತಾಗಿತ್ತು. ನಂತರ ೨೦೦೩, ಫ಼ೆಬ್ರವರಿ ೬ ನೇ ದಿನಾಂಕದಿಂದ ಚೆಕ್ಕುಗಳನ್ನು ಕೂಡ ಈ ಕಾಯಿದೆಯಲ್ಲಿ ಸೇರಿಸಲಾಯಿತು.

ಕಾನೂನಿನ ಭೌಗೋಳಿಕ ವ್ಯಾಪ್ತಿ

ಮಾತಂಕಾ, ಸೆಕ್ಷನ್ ೧ ರ ಪ್ರಕಾರ ಈ ಕಾನೂನು ಜಮ್ಮು ಮತ್ತು ಕಾಶ್ಮೀರವನ್ನು ಸೇರಿ ಭಾರತದ ಎಲ್ಲಾ ಪ್ರದೇಶಗಳಿಗೂ ಅನ್ವಯವಾಗುತ್ತದೆ. ಅಲ್ಲದೆ ಸೆಕ್ಷನ್ ೭೫ ರ ಪ್ರಕಾರ ಈ ಕಾನೂನಿನಲ್ಲಿ ಉಲ್ಲೇಖಿಸಿರುವ ಯಾವುದೇ ಅಪರಾಧದಲ್ಲಿ ಭಾರತದಲ್ಲಿರುವ ಯಾವುದೇ ಕಂಪ್ಯೂಟರ್ ಭಾಧಿಸಲ್ಪಟ್ಟಿದ್ದರೆ, ಅಪರಾಧಿ ಭಾರತದ ಹೊರಗಡೆ ಇದ್ದರೂ ಅಥವಾ, ಅವನು ವಿದೇಶಿ ವ್ಯಕ್ತಿಯಾಗಿದ್ದರೂ ಅವನು ಈ ಕಾನೂನಿನ ವ್ಯಾಪ್ತಿಯೊಳಗಡೆ ಬರುತ್ತಾನೆ.

ಗಣಕ ಪತ್ರ ಧೃಢೀಕರಣ

ಸೆಕ್ಷನ್ ೪ ರ ಪ್ರಕಾರ ಯಾವುದೇ ಗಣಕ ಪತ್ರ, ಬರವಣಿಗೆ ಪತ್ರಕ್ಕೆ ಸಮ. ನಾವು ಬರವಣಿಗೆಯ ಪತ್ರಕ್ಕೆ ಸಹಿಯ ಮೂಲಕವಾಗಿಯಾಗಲೀ ಅಥವಾ ಹೆಬ್ಬೆಟ್ಟಿನ ಗುರುತಿನಿಂದಾಗಲೀ ಧೃಢೀಕರಣ ಮಾಡುವಂತೆ ಗಣಕ ಪತ್ರಕ್ಕೆ ಸಹಿ ಮಾಡುವ ವಿಧಾನವನ್ನು ಮಾತಂಕಾ ೨೦೦೦ ದ ಸೆಕ್ಷನ್ ೩ ರಲ್ಲಿ ಉಲ್ಲೇಖಿಸಲಾಗಿದೆ. ಇದಕ್ಕೆ ''ಡಿಜಿಟಲ್ ಸಹಿ'' ಎಂದು ಹೆಸರು.

ಅದರೊಂದಿಗೆ ಸೆಕ್ಷನ್ ೫ ರ ಪ್ರಕಾರ ಭಾರತದ ಯಾವುದೇ ಕಾನೂನಿನಲ್ಲಿ "ಸಹಿ" ಮಾಡುವ ಅವಶ್ಯಕತೆ ತಿಳಿಸಲ್ಪಟ್ಟಿದ್ದರೆ, ಆ ಅವಶ್ಯಕತೆಯನ್ನು "ಡಿಜಿಟಲ್ ಸಹಿ" ಮೂಲಕ ಪೂರೈಸಬಹುದು.

ಮಾತಂಕಾ ೨೦೦೦ ದಲ್ಲಿ ಗಣಕ ಪತ್ರಗಳ ಧೃಢೀಕರಣವನ್ನು ಮಾಡುವ ಬೇರಾವುದೇ ವಿಧಾನವನ್ನು ಉಲ್ಲೇಖಿಸಿಲ್ಲವಾದ್ದರಿಂದ "ಡಿಜಿಟಲ್ ಸಹಿ" ಇಲ್ಲದ ಗಣಕ ದಾಖಲೆಗಳೆಲ್ಲಾ ಬರವಣಿಗೆಯಲ್ಲಿದ್ದರೂ ಕೂಡ ಅದು ಕಾನೂನಿನ ದೃಷ್ಟಿಯಲ್ಲಿ "ಬಾಯಿ ಮಾತಿನ ಸಾಕ್ಷಿ" ಯಂತೆ ಪರಿಗಣಿಸಲ್ಪಡುತ್ತದೆಯೇ ಹೊರತು ಬರವಣಿಗೆ ಪತ್ರವೆಂದು ಪರಿಗಣಿಸಲ್ಪಡುವುದಿಲ್ಲ.

ಅನೇಕ ವೆಬ್ ಸೈಟ್ ಗಳಲ್ಲಿ ಇಂದು ಪಾಸ್‌ವರ್ಡನ್ನು ಗುರುತಿನ ಸಂಕೇತವಾಗಿ ಬಳಸುವುದು ರೂಢಿಯಲ್ಲಿದೆ. ಒಮ್ಮೆ ವೆಬ್‌ಸೈಟ್ ಗ್ರಾಹಕನೊಬ್ಬನನ್ನು ಪಾಸ್‌ವರ್ಡ್ ಮೂಲಕ ಗುರುತಿಸಿ ಅವನು ವೆಬ್‌ಸೈಟ್ ಒಳಗೆ ಬಂದ ನಂತರ ಡಿಜಿಟಲ್ ಸಹಿ ಇಲ್ಲದೆ ಅವನ ಅಪ್ಪಣೆಯನ್ನು ಬೇರೆ ವ್ಯವಹಾರಕ್ಕೆ ಬಳಸಿದರೆ ಅದು ಕಾನೂನಿನ ಪ್ರಕಾರ ಸರಿಯಾಗುವುದಿಲ್ಲ. ಆದರೂ ಇಂದು ಅನೇಕ ಬ್ಯಾಂಕು ಹಾಗೂ ಸರ್ಕಾರದ ವೆಬ್ ಸೈಟ್ ಗಳಲ್ಲಿ ಪಾಸ್ ವರ್ಡನ್ನೇ ಗಣಕ ಪತ್ರದ ಧೃಡೀಕರಣಕ್ಕೆ ಉಪಯೋಗಿಸುವ ತಪ್ಪು ಸಂಪ್ರದಾಯ ನಡೆದು ಬಂದಿದೆ. ಇದನ್ನು ಶ್ರೀಘ್ರವಾಗಿ ಸರಿಪಡಿಸದೇ ಹೋದರೆ ಗ್ರಾಹಕರು ಕಾನೂನಿನ ತೊಂದರೆಗೆ ಸಿಲುಕುವುದು ಖಚಿತ.

ಡಿಜಿಟಲ್ ಸಹಿ

ಸೆಕ್ಷನ್ ೩ ರ ಪ್ರಕಾರ ಡಿಜಿಟಲ್ ಸಹಿ ಎಂಬುದು ಒಂದು ಗಣಕ ಪ್ರಕ್ರಿಯೆ. ಇದರ ಮೂಲಕ ಸಹಿ ಮಾಡುವವರು ಗಣಕ ದಾಖಲೆಯ ಮೇಲೆ ತಮ್ಮದೇ ಆದ ಮುದ್ರೆ ಒತ್ತಬಹುದು. ಅಲ್ಲದೆ, ಈ ಮುದ್ರೆ ಒತ್ತಿದ ಬಳಿಕ ದಾಖಲೆಗೆ ಯಾವರೀತಿಯ ಬದಲಾವಣೆಯೂ ಆಗಿಲ್ಲ ಎಂಬುದನ್ನು ಖಾತ್ರಿ ಮಾಡಬಹುದು. ವೈಯುಕ್ತಿಕ ಮುದ್ರೆ ಮತ್ತು ಮಾಹಿತಿ ಖಾತ್ರಿ ಎರಡನ್ನೂ ಡಿಜಿಟಲ್ ಸಹಿ ಒದಗಿಸುವುದರಿಂದ

ಕಾನೂನಿನಲ್ಲಿ ಡಿಜಿಟಲ್ ಸಹಿಗೆ ಮಹತ್ವದ ಬೆಲೆಯನ್ನು ನೀಡಲಾಗಿದೆ. ಅದರ ಪ್ರಕಾರ ಡಿಜಿಟಲ್ ಸಹಿ ಇರುವ ಯಾವುದೇ ಗಣಕ ಪತ್ರ ಬೇರೆ ಯಾವ ಸಾಕ್ಷಿಯೂ ಇಲ್ಲದೆ ಸಹಿ ಮಾಡಿದವನ ವಿರುದ್ಧ ಸಾಕ್ಷಿ ಎಂದು ಪರಿಗಣಿಸಲ್ಪಡುತ್ತದೆ.

ಈ ಡಿಜಿಟಲ್ ಸಹಿ ನಾವು ತಿಳಿದಿರುವ ಬರವಣಿಗೆ ಸಹಿ ಅಥವಾ ಬೆರಳಚ್ಚು ಸಹಿ ಗೆ ಭಿನ್ನ ಎಂಬುದನ್ನು ನಾವು ತಿಳಿಯಬೇಕು.

ಸಹಿದಾರ ತನ್ನ ಹೆಸರನ್ನು ಬರೆದು ಅದನ್ನು ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿ ಚಿತ್ರಿಸಿದರೆ ಅದು ಡಿಜಿಟಲ್ ಸಹಿ ಆಗುವುದಿಲ್ಲ ಎಂಬ ವಿಚಾರವನ್ನು ಕೂಡ ನಾವು ಮನದಟ್ಟು ಮಾಡಿಕೊಳ್ಳಬೇಕು.

ಹಾಗೆಯೇ, ಡಿಜಿಟಲ್ ಸಹಿ ಎಂಬುದು ದಾಖಲೆ ಯಿಂದ ದಾಖಲೆಗೆ ಬದಲಾವಣೆಯಾಗುತ್ತದೆಯೆಂಬ ಸತ್ಯವನ್ನೂ ತಿಳಿದಿರಬೇಕು.

ಡಿಜಿಟಲ್ ಸಹಿ ಎರಡು ಅಂಶಗಳನ್ನು ಹೊಂದಿರುತ್ತದೆ. ಮೊದಲನೆಯದು ದಾಖಲೆಯ ''ಸಂಕ್ಷಿಪ್ತ ಸೂಚಕ''. ಇದನ್ನು ''ಹ್ಯಾಶ್ ಕೋಡ್'' ಎಂದು ಕರೆಯುತ್ತಾರೆ. ಈ ಸಂಕ್ಷಿಪ್ತ ಸೂಚಕ ಯಾವುದೇ ಗಣಕ ದಾಖಲೆಯನ್ನು ಒಂದು ಸೂಚ್ಯಂಕ ವಾಗಿ ಪರಿವರ್ತಿಸುತ್ತದೆ. ಡಿಜಿಟಲ್ ಸಹಿಯಲ್ಲಿ ಉಪಯೋಗಿಸುವ ಎಂಡಿ ೫ ಮತ್ತು ಶಾ ೧ ಎಂಬ ಸೂಚ್ಯಂಕ ಗಣಿತ ಯಾವುದೇ ದಾಖಲೆಯಲ್ಲಿ ಒಂದು ಚುಕ್ಕೆ ಬದಲಾವಣೆಯಾದರೂ ಅದರ ಸೂಚ್ಯಂಕ ಬದಲಾವಣೆಯಾಗುವಂತಹ ಪ್ರವೃತ್ತಿಯನ್ನು ಹೊಂದಿರುತ್ತದೆ. ಹಾಗೆಯೇ ಯಾವುದೇ ದಾಖಲೆಯ ಸೂಚ್ಯಂಕವನ್ನು ಮತ್ತೆ ಮತ್ತೆ ಕಂಡು ಹಿಡಿದರೂ ಅದೂ ಪ್ರತಿ ಬಾರಿಯೂ ಒಂದೇ ಸೂಚ್ಯಂಕವನ್ನು ತೋರಿಸುತ್ತದೆ.

ಅಲ್ಲದೆ ಈ ಸಂಕ್ಷಿಪ್ತ ಸೂಚಕಗಳು ಏಕ ಮುಖ ಸೂಚಕಗಳಾಗಿದ್ದು, ದಾಖಲೆಯೊಂದರಿಂದ ಅದರ ಸೂಚ್ಯಂಕವನ್ನು ಕಂಡು ಹಿಡಿಯಬಹುದೇ ಹೊರತು, ಸೂಚ್ಯಂಕವೊಂದರಿಂದ ದಾಖಲೆಯನ್ನು ಸೃಷ್ಟಿಸಲು ಬರುವುದಿಲ್ಲ.

ಈ ಸಂಕ್ಷಿಪ್ತ ಸೂಚಕ, ಡಿಜಿಟಲ್ ಸಹಿಯಲ್ಲಿ ದಾಖಲೆಯ ಮಾಹಿತಿ ಬದಲಾವಣೆಯನ್ನು ಕಂಡುಹಿಡಿಯಲು ಉಪಯೋಗಿಸಲಾಗಿದೆ.

ಡಿಜಿಟಲ್ ಸಹಿಯ ಎರಡನೇ ಅಂಶವೆಂದರೆ ''ಅಸಮಾನ ಗೌಪ್ಯ ಸಂದೇಶ'' (ಅಸಿಮೆಟ್ರಿಕ್ ಕ್ರಿಪ್ಟೊ ಸಿಸ್ಟಮ್). ಅಸಮಾನ ಗೌಪ್ಯ ಸಂದೇಶ ವಾಹಿನಿ ಎರಡು ಕೀಲಿ ಇರುವ ಬೀಗದಂತೆ. ಒಂದು ಕೀಲಿ ಜೋಡಿಯ ಒಂದು ಕೀಲಿಯಿಂದ ದಾಖಲೆಯೊಂದನ್ನು ಗೌಪ್ಯ ಪಡಿಸಿದರೆ (ಅಥವಾ ಮುಚ್ಚಿದರೆ) , ಅದನ್ನು ಅಗೌಪ್ಯ ಪಡಿಸಲು (ಅಥವಾ ತೆರೆಯಲು) ಜೋಡಿ ಕೀಲಿಯಿಂದ ಮಾತ್ರ ಸಾಧ್ಯ.

ಇದರಿಂದ ಯಾವುದೇ ಗೌಪ್ಯ ದಾಖಲೆಯನ್ನು ಯಾವುದೇ ಕೀಲಿಯಿಂದ ತೆರೆಯಲು ಸಾಧ್ಯವಾದರೆ ಅದನ್ನು ಆ ಕೀಲಿಯ ಜೋಡಿಯಿಂದಲೇ ಗೌಪ್ಯ ಪಡಿಸಲಾಗಿತ್ತೆಂದು ಖಚಿತವಾಗಿ ಹೇಳಬಹುದು.

ಡಿಜಿಟಲ್ ಸಹಿ ತಂತ್ರದಲ್ಲಿ ಮಾಡುವುದೇನೆಂದರೆ, ದಾಖಲೆಯ ಸಂಕ್ಷಿಪ್ತ ಸೂಚ್ಯಂಕವನ್ನು ಮೊದಲು ಕಂಡು ಹಿಡಿದು ಅದನ್ನು ಒಂದು ಜೋಡಿ ಕೀಲಿಯಿಂದ ಮುಚ್ಚುವುದು. ಈ ಮುಚ್ಚಿದ ಸೂಚ್ಯಂಕವನ್ನು ದಾಖಲೆಯ ಜೊತೆ ಸೇರಿಸಿ ಇಡುವುದು.

ನಂತರ ಬೇರೆಯವರು ದಾಖಲೆಯನ್ನು ಧೃಡೀಕರಿಸಿದವರು ಯಾರೆಂದು ತಿಳಿದುಕೊಳ್ಳಬೇಕಾದರೆ, ಅವರು ಜೋಡಿ ಕೀಲಿಯ ಇನ್ನೊಂದು ಕೀಲಿಯಿಂದ ಸೂಚ್ಯಂಕವನ್ನು ಅಗೌಪ್ಯ ಗೊಳಿಸಲು ಪ್ರಯತ್ನ ಪಡಬೇಕು. ಇದು ಸಾಧ್ಯವಾದರೆ, ಈ

ಅಗೌಪ್ಯ ಕೀಲಿ ಮಾಲಿಕನೇ ಆ ದಾಖಲೆಯ ಸೃಷ್ಟಿಕರ್ತ ಎಂದು ತಿಳಿಯಬೇಕು. ನಂತರ ದಾಖಲೆಯು ಬದಲಾಯಿಸಲ್ಪಟ್ಟಿಲ್ಲ ಎಂದು ತಿಳಿಯುವುದಕ್ಕೆ ತಮ್ಮ ಬಳಿ ಇರುವ ದಾಖಲೆಯ ಸಂಕ್ಷಿಪ್ತ ಸೂಚ್ಯಂಕವನ್ನು ಮತ್ತೆ ಕಂಡು ಹಿಡಿದು ದಾಖಲೆಯ ಜೊತೆ ನಮೂದಿಸಲಾದ ಸೂಚ್ಯಂಕಕ್ಕೆ ಹೊಂದುತ್ತದೆಯೇ ಎಂದು ಪರೀಕ್ಷಿಸಬೇಕು. ಈ ದ್ವಿಪ್ರಕ್ರಿಯೆಯ ಮೂಲಕ ಯಾವುದೇ ಗಣಕ ದಾಖಲೆಯ ಧೃಡೀಕರಣ ಮಾಡಬಹುದು.

ಈ ರೀತಿಯ ವ್ಯವಸ್ಥೆಯ ಉಪಯೋಗಕ್ಕೆ ಎರಡು ಕೀಲಿಗಳಲ್ಲಿ ಒಂದನ್ನು ಸಾರ್ವಜನಿಕ ಕೀಲಿಯೆಂದೂ, ಇನ್ನೊಂದನ್ನು ವೈಯುಕ್ತಿಕ ಕೀಲಿಯೆಂದೂ ಪರಿಗಣಿಸಲಾಗುತ್ತದೆ. ಇದರಲ್ಲಿ ವೈಯುಕ್ತಿಕ ಕೀಲಿ ಯಾವಾಗಲೂ ಸಹಿ ಮಾಡುವವರ ಬಳಿಯೇ ಇರುತ್ತದೆ. ಸಾರ್ವಜನಿಕ ಕೀಲಿಯನ್ನು ಎಲ್ಲರಿಗೂ ಕೊಡಲಾಗುತ್ತದೆ.

ಈ ವ್ಯವಸ್ಥೆಯನ್ನು ನಿರ್ವಹಿಸಲು ಮಾತಂಕಾ ೨೦೦೦ ದಲ್ಲಿ ವಿವರವಾದ ಸೂಚನೆಗಳನ್ನು ಕೊಡಲಾಗಿದೆ. ಇದರ ಪ್ರಕಾರ ಯಾವುದೇ ವ್ಯಕ್ತಿ ಡಿಜಿಟಲ್ ಸಹಿಯನ್ನು ಕಾನೂನಿನ ಪ್ರಕಾರ ಗಣಕ ದಾಖಲೆಯ ಧೃಡೀಕರಣಕ್ಕೆ ಉಪಯೋಗಿಸಬೇಕಾದರೆ ಅವನು ಲೈಸೆನ್ಸ್ ಪಡೆದ ಸರ್ಟಿಫ್ಲೈಯಿಂಗ್ ಅಥಾರಿಟಿ (ಪ್ರಮಾಣ ಪೀಠ) ಯಿಂದ ಡಿಜಿಟಲ್ ಸರ್ಟಿಫಿಕೇಟ್ ಎಂಬ ಪರವಾನಿಗೆ ಪತ್ರವನ್ನು ಪಡೆಯಬೇಕು. ಈ ಪರವಾನಿಗೆ ಪತ್ರ ಕೊಡುವ ಮುನ್ನ ಪ್ರಮಾಣ ಪೀಠ ಸಹಿ ಮಾಡುವವನ ಅಧಿಕೃತ ದಾಖಲೆಗಳನ್ನು ಪರಿಶೀಲಿಸಿ ಅವನ ಹೆಸರು ಮತ್ತು ವಿಳಾಸವನ್ನು ಪರೀಕ್ಷಿಸಬಹುದು.

ಆನಂತರ, ಅರ್ಜಿದಾರ ಪ್ರಮಾಣ ಪೀಠ ದ ವೆಬ್ ಸೈಟ್ ಗೆ ಹೋಗಿ ಒಂದು ಕೀಲಿ ಜೋಡಿಯನ್ನು ತಾನೇ ಸೃಷ್ಟಿಸಿ, ವೈಯುಕ್ತಿಕ ಕೀಲಿಯನ್ನು ತನ್ನ ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿ ಅಡಗಿಸಿಟ್ಟು ಸಾರ್ವಜನಿಕ ಕೀಲಿಯನ್ನು ಪ್ರಮಾಣ ಪೀಠಕ್ಕೆ ಸರ್ಟಿಫಿಕೇಟ್

ಕೊಡುವುದಕ್ಕಾಗಿ ಕಳುಹಿಸಿ ಅದನ್ನು ಡಿಜಿಟಲ್ ಸರ್ಟಿಫ಼ಿಕೇಟ್ ರೂಪದಲ್ಲಿ ಹಿಂದಕ್ಕೆ ಪಡೆಯುತ್ತಾನೆ.

ಈ ಡಿಜಿಟಲ್ ಸರ್ಟಿಫ಼ಿಕೇಟ್ ಎಂಬುದು, ಒಂದು ಪರವಾನಿಗೆ ಇದ್ದ ಹಾಗೆ. ಇದರಲ್ಲಿ ಸಹಿದಾರನ ಸಾರ್ವಜನಿಕ ಕೀಲಿಯಲ್ಲದೆ, ''ಇದು ಇಂತಹವರ ಸಾರ್ವಜನಿಕ ಕೀಲಿ. ಇದು ಇಂತಹ ದಿನಾಂಕದ ವರೆಗೆ ಚಾಲ್ತಿಯಲ್ಲಿರುತ್ತದೆ'' ಎಂಬ ಪ್ರಮಾಣ ವನ್ನು ಕೂಡ ಒಳಗೊಂಡಿರುತ್ತದೆ.

ಈ ಡಿಜಿಟಲ್ ಸರ್ಟಿಫ಼ಿಕೇಟ್ ನ ಒಂದು ಪ್ರತಿಯನ್ನು ಪ್ರಮಾಣ ಪೀಠ ಸಾರ್ವಜನಿಕ ಸಂಗ್ರಹಾಲಯ ದಲ್ಲಿ ಇಡುತ್ತದೆ. ಇದನ್ನು ಸಾರ್ವಜನಿಕರಾರಾದರೂ ಪಡೆಯಬಹುದು. ಅಲ್ಲದೆ, ಸರ್ಟಿಫ಼ಿಕೇಟ್ ಹೊಂದಿರುವವರು ಅದನ್ನು ಯಾರಿಗಾದರೂ ಕಳುಹಿಸಿಕೊಡಬಹುದು. ಈ ಸರ್ಟಿಫ಼ಿಕೇಟ್ ಇದ್ದವರಲ್ಲಿ ಸಹಿದಾರನ ಸಾರ್ವಜನಿಕ ಕೀಲಿ ಇರುವುದರಿಂದ ಅವರು ಸಹಿದಾರನು ಸಹಿ ಮಾಡಿದ ಯಾವುದೇ ದಾಖಲೆಯನ್ನಾದರೂ ಪರೀಕ್ಷೆ ಮಾಡಿ ಇದನ್ನು ಇಂತಹವರೇ ಸಹಿ ಮಾಡಿದ್ದಾರೆಂದು ತಿಳಿಯಬಹುದು.

ಈ ಪ್ರಮಾಣ ಪೀಠಗಳಿಗೆಲ್ಲಾ ಮೂಲವಾಗಿ ಮಾತಂಕಾ ೨೦೦೦ ದ ಅನ್ವಯ, ಭಾರತ ದೇಶಕ್ಕೆಲ್ಲಾ ''ಕಂಟ್ರೋಲರ್ ಆಫ಼್ ಸರ್ಟಿಫ಼್ಯೈಯಿಂಗ್ ಅಥಾರಿಟೀಸ್'' ಎಂಬ ಅಧಿಕಾರಿ ನೇಮಕಪಟ್ಟಿದ್ದಾರೆ. ಪ್ರಮಾಣ ಪೀಠಗಳು ಈ ಕಂಟ್ರೋಲರ್ ರವರಿಂದ ಅನುಮತಿ ಪಡೆದರೆ ಮಾತ್ರ ಅವರುಗಳು ನೀಡುವ ಡಿಜಿಟಲ್ ಸರ್ಟಿಫ಼ಿಕೇಟ್ ಗಳು ಭಾರತ ಕಾನೂನಿನಲ್ಲಿ ಒಪ್ಪಿಗೆಯಾಗುತ್ತವೆ. ಅಂತಹ ಡಿಜಿಟಲ್ ಸರ್ಟಿಫ಼ಿಕೇಟ್ ಗಳನ್ನು ಉಪಯೋಗಿಸಿ ಮಾಡಿದ ಡಿಜಿಟಲ್ ಸಹಿ ಮಾತ್ರವೇ ಮಾತಂಕಾ ಕಾನೂನಿನ ಪ್ರಕಾರ ಊರ್ಜಿತವಾಗುತ್ತದೆ.

ಇದುವರೆಗೆ ಭಾರತದಲ್ಲಿ ಆರು ಪ್ರಮಾಣ ಪೀಠ ಗಳಿಗೆ ಲೈಸೆನ್ಸ್ ಕೊಡಲಾಗಿದೆ. ಅವುಗಳಲ್ಲಿ ಎನ್.ಐ.ಸಿ. ಎಂಬ ಸರ್ಕಾರಿ ಸ್ವಾಮ್ಯದ ಸಂಸ್ಥೆ ಸರ್ಕಾರಿ ಕರ್ಮಚಾರಿಗಳಿಗೆ ಮಾತ್ರ ಮೀಸಲಾಗಿದೆ. ಐ.ಡಿ.ಆರ್.ಬಿ.ಟಿ. ಎಂಬ ರಿಸರ್ವ್ ಬ್ಯಾಂಕ್ ನ ಘಟಕ ಬ್ಯಾಂಕ್ ಉದ್ಯೋಗಿಗಳಿಗೆ ಸರ್ಟಿಫ಼ಿಕೇಟ್ ಕೊಡುವುದಕ್ಕೆ ಸೀಮಿತವಾಗಿದೆ. ಸಾರ್ವಜನಿಕರಿಗೆ ಸೇಫ಼್ ಸ್ಕ್ರಿಪ್ಟ್, ಟಿ.ಸಿ.ಎಸ್. ಎಂ.ಟಿ.ಎನ್.ಎಲ್., ಮತ್ತು ಎನ್ ಕೋಡ್ ಸಲ್ಯೂಶನ್ಸ್, ಸಂಸ್ಥೆಗಳು ಸರ್ಟಿಫ಼ಿಕೇಟ್‌ಗಳನ್ನು ನೀಡಲು ಪರವಾನಿಗೆ ಪಡೆದಿವೆ. ಈ ರೀತಿಯ ಸರ್ಟಿಫ಼ಿಕೇಟ್‌ಗಳು ವರ್ಷಕ್ಕೆ ರೂ ೫೦೦ ರಿಂದ ೫೦೦೦ ದ ವರೆಗಿನ ಖರ್ಚಿನಲ್ಲಿ ವಿವಿಧುಗೆಯಾಗಿ ದೊರೆಯುತ್ತವೆ.

ಡಿಜಿಟಲ್ ಸರ್ಟಿಫ಼ಿಕೇಟ್ ಕೊಳ್ಳುವ ಮುನ್ನ ಗ್ರಾಹಕರು ಕೆಲವು ರೀತಿಯ ಎಚ್ಚರವನ್ನು ವಹಿಸಬೇಕಾದುದು ಅಗತ್ಯ.ಆವುಗಳೇನೆಂದರೆ,

೧. ಡಿಜಿಟಲ್ ಸರ್ಟಿಫ಼ಿಕೇಟ್ ಗೆ ಅರ್ಜಿ ನೀಡುವಾಗ ತಪ್ಪು ಹೆಸರು ಅಥವಾ ವಿಳಾಸ ನೀಡಬಾರದು. ತಪ್ಪು ಮಾಹಿತಿ ಇತ್ತು ಸರ್ಟಿಫ಼ಿಕೇಟ್ ಪಡೆಯುವುದು ಅಥವಾ, ಸರ್ಟಿಫ಼ಿಕೇಟ್ ಗಳ ತಪ್ಪು ಉಪಯೋಗ ಮಾಡುವುದು, ಮಾತಂಕಾ ಪ್ರಕಾರ ಶಿಕ್ಷಾರ್ಹ ಅಪರಾಧ ವಾಗುತ್ತದೆ. ಇದಕ್ಕೆ ೨ ವರ್ಷ ಸೆರೆಮನೆ ವಾಸ ಮತ್ತು ರೂಪಾಯಿ ೧ ಲಕ್ಷ ದಂಡ ವಿಧಿಸಲು ಅವಕಾಶವಿರುತ್ತದೆ.

೨. ಡಿಜಿಟಲ್ ಸರ್ಟಿಫ಼ಿಕೇಟ್ ಪಡೆದ ವ್ಯಕ್ತಿ ತನ್ನ ವೈಯುಕ್ತಿಕ ಕೀಲಿಯನ್ನು ಭದ್ರವಾಗಿಟ್ಟುಕೊಳ್ಳಬೇಕು. ಅಕಸ್ಮಾತ್ ಈ ವೈಯುಕ್ತಿಕ ಕೀಲಿ ಬೇರೆಯವರಿಗೆ ಸಿಕ್ಕಿರುವ ಸಂಶಯ ಬಂದರೆ ಈ ವಿಷಯವನ್ನು ಪ್ರಮಾಣ ಪೀಠಕ್ಕೆ ಒಡನೆಯೇ ತಿಳಿಸಿ ಬೇರೆ ಕೀಲಿಯನ್ನು ಅವನು ಪಡೆಯಬೇಕು. ಇಲ್ಲದಿದ್ದರೆ ಕಳೆದು ಹೋದ ಕೀಲಿಯನ್ನು ಉಪಯೋಗಿಸಿ ಮಾಡಿದ ವ್ಯವಹಾರಗಳಿಗೆ ಅವನು ಭಾಧ್ಯನಾಗುತ್ತಾನೆ.

೩. ಗ್ರಾಹಕರು ಡಿಜಿಟಲ್ ಸಹಿ ಮಾಡಬೇಕಾದಾಗ ವೈಯುಕ್ತಿಕ ಕೀಲಿಯನ್ನು ಪ್ರಯೋಗಮಾಡಬೇಕಾಗುತ್ತದೆ. ಈ ಸಂದರ್ಭಗಳಲ್ಲಿ ಸಹಿಯನ್ನು ಉಪಯೋಗಿಸುವ ತಂತ್ರಾಂಶ (ಉದಾಹರಣೆಗೆ: ಇ–ಮೈಲ್ ಕಳುಹಿಸುವ ಔಟ್ ಲುಕ್ ಎಕ್ಸ್‌ಪ್ರೆಸ್ ಅಥವಾ ಬರವಣಿಗೆಗೆ ಉಪಯೋಗಿಸುವ ವರ್ಡ್) ಕಂಪ್ಯೂಟರ್ ನಲ್ಲೆಲ್ಲೋ ಹುಗಿದಿಟ್ಟಿರುವ ಕೀಲಿಯನ್ನು ಹೊರ ತೆಗೆದು ಉಪಯೋಗಿಸುತ್ತದೆ. ಈ ರೀತಿ ವೈಯುಕ್ತಿಕ ಕೀಲಿಯನ್ನು ಉಪಯೋಗಿಸುವ ಪ್ರತಿ ಬಾರಿಯೂ ತಂತ್ರಾಂಶ ಗುರುತಿನ ಪಾಸ್ ವರ್ಡ್ ಕೇಳುವ ರೀತಿ ಮಾಡಬೇಕು. ಇಲ್ಲದಿದ್ದರೆ ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಉಪಯೋಗಿಸುವ ಬೇರೆ ಯಾರಾದರೂ, ನಿಮ್ಮ ಸಹಿಯನ್ನು ಉಪಯೋಗಿಸಿ ದಾಖಲೆಗಳಿಗೆ ನಿಮ್ಮ ಸಹಿ ಇರುವಂತೆ ಫ್ಲೋರ್ಜರಿ ಮಾಡಬಹುದು. ಒಂದೇ ಕಂಪ್ಯೂಟರನ್ನು ಹಲವರು ಉಪಯೋಗಿಸುವ ಸಂದರ್ಭವಿದ್ದಲ್ಲಿ ವೈಯುಕ್ತಿಕ ಕೀಲಿಯನ್ನು ಕಂಪ್ಯೂಟರ್ ನಲ್ಲಿ ಉಳಿಸದೆ, ಅದನ್ನು ಫ್ಲಾಪ್ಪಿ ಅಥವಾ ಸಿ.ಡಿ ಮೂಲಕ ಮಾತ್ರ ಉಪಯೋಗಿಸುವ ಹಾಗೆಯೋ ಅಥವಾ ಸ್ಮಾರ್ಟ್ ಕಾರ್ಡ್ ಮೂಲಕ ಉಪಯೋಗಿಸುವಂತೆಯೋ ವ್ಯವಸ್ಥೆ ಮಾಡಿಕೊಳ್ಳಬೇಕು.

೪. ವೈಯುಕ್ತಿಕ ಕೀಲಿ ಪ್ರಯೋಗಕ್ಕೆ ಪಾಸ್ ವರ್ಡ್ ಉಪಯೋಗಿಸಿದರೆ ಆ ಪಾಸ್‌ವರ್ಡನ್ನು ಬಹಳ ಎಚ್ಚರದಿಂದ ಕಾಪಾಡಿಕೊಳ್ಳಬೇಕು. ಯಾವುದೇ ಕಾರಣಕ್ಕೂ ಅದನ್ನು ಬೇರೆಯವರಿಗೆ ತಿಳಿಸುವುದು ಸಹಿ ಮಾಡಿದ ಖಾಲಿ ಚೆಕ್ ಬೇರೆಯವರಿಗೆ ಕೊಟ್ಟಂತೆ ಎಂದು ಭಾವಿಸಿಕೊಳ್ಳಬೇಕು.

ಇ–ಆಡಳಿತ

ಸರ್ಕಾರಿ ಆಡಳಿತದಲ್ಲಿ ಗಣಕ ದಾಖಲೆಗಳ ಉಪಯೋಗಕ್ಕೆ ಕಾನೂನಿನ ಅಡಚಣೆ ಇರದಂತೆ ಮಾತಂಕಾ ೨೦೦೦ ದಲ್ಲಿ ಸೆಕ್ಷನ್ ೬,೭,೮ ರ ಮೂಲಕ ಸರ್ಕಾರಿ ಘಟಕಗಳಿಗೆ ಹಾಗೂ ಸರ್ಕಾರಿ ಸ್ವಾಮ್ಯದ ಸಂಸ್ಥೆಗಳಿಗೆ ಅನುಮತಿ ನೀಡಲಾಗಿದೆ.

ಇದರ ಪ್ರಕಾರ ಸರ್ಕಾರಕ್ಕೆ ಯಾವುದೇ ಅರ್ಜಿ ಸಲ್ಲಿಸಲು, ಅಥವಾ ಟೆಂಡರ್ ವ್ಯವಹಾರದಲ್ಲೂ ಗಣಕ ಪತ್ರಗಳ ಬಳಕೆಗೆ ಅವಕಾಶ ಮಾಡಬಹುದು. ಹಾಗೆಯೇ, ಹಣ ಪಡೆಯುವುದಕ್ಕೆ ಅಥವಾ ಕೊಡುವುದಕ್ಕೆ ಮತ್ತು ಸರ್ಕಾರಿ ದಾಖಲೆಗಳನ್ನು ಉಳಿಸಿಟ್ಟುಕೊಳ್ಳುವುದಕ್ಕೆ ಕೂಡ ಗಣಕ ದಾಖಲೆಗಳನ್ನು ಉಪಯೋಗಿಸಬಹುದು. ಸರ್ಕಾರಿ ಗೆಜ಼ೆಟ್ ಕೂಡಾ ಗಣಕ ಪತ್ರದ ಮೂಲಕ ಹೊರಡಿಸುವುದಕ್ಕೆ ಕೂಡ ಈ ಮೂಲಕ ಅವಕಾಶ ಕೊಡಲಾಗಿದೆ.

ಮೇಲ್ಕಂಡಂತೆ ಸರ್ಕಾರದ ಅನೇಕ ವ್ಯವಹಾರಗಳಲ್ಲಿ ಗಣಕ ಯಂತ್ರದ ಬಳಕೆ ಸಾಧ್ಯವಾದರೂ, ಸೆಕ್ಷನ್ ೯ ರ ಪ್ರಕಾರ ಸರ್ಕಾರದಲ್ಲಿ ಗಣಕ ಪತ್ರದ ಬಳಕೆ ಮಾಡುವುದಕ್ಕೆ ಸಾರ್ವಜನಿಕರಿಗೆ ಒತ್ತಾಯ ಮಾಡುವ ಹಕ್ಕು ಇಲ್ಲ ಎಂದು ತಿಳಿಸಲಾಗಿದೆ. ಇದರಿಂದ ಸರ್ಕಾರಿ ಘಟಕಗಳು ತಮ್ಮದೇ ವೇಗದಲ್ಲಿ ಗಣಕ ಯಂತ್ರದ ಬಳಕೆಯನ್ನು ಒಳಗೂಡಿಸಿಕೊಳ್ಳಲು ಅವಕಾಶ ಮಾಡಿಕೊಡಲಾಗಿದೆ.

ಮಾತಂಕಾ–೨೦೦೦ ದ ಅಂಶಗಳನ್ನು ಅನುಷ್ಠಾನಗೊಳಿಸಲು ರಾಜ್ಯ ಸರ್ಕಾರಗಳು ಬೇಕಾದ ನಿಯಮಗಳನ್ನು ಮಾಡಲು ಸೆಕ್ಷನ್ ೯೦ ರ ಪ್ರಕಾರ ಅನುಮತಿ ಕೊಡಲಾಗಿದೆ.

ಅಪರಾಧಗಳು

ನಾವು ಈಗಾಗಲೇ ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳ ಬಗ್ಗೆ ಚರ್ಚಿಸಿದ್ದೇವೆ. ಈಗ ಸಂಕ್ಷಿಪ್ತವಾಗಿ ಮಾತಂಕಾ ೨೦೦೦ ದಲ್ಲಿ ಅಪರಾಧಗಳ ಬಗ್ಗೆ ಇರುವ ಕಾನೂನನ್ನು ಅವಲೋಕಿಸೋಣ.

ಮಾತಂಕಾ–೨೦೦೦, ಅಪರಾಧಗಳನ್ನು ಎರಡು ವಿಧದಲ್ಲಿ ವಿಂಗಡಿಸಿದೆ. ಅದರಂತೆ, ಮಾತಂಕಾ ದ ೯ನೇ ವಿಭಾಗ ದಲ್ಲಿ ಸಿವಿಲ್ ರೂಪದ ಅಪರಾಧಗಳನ್ನೂ, ೧೧ನೇ ವಿಭಾಗದಲ್ಲಿ ಕ್ರಿಮಿನಲ್ ರೂಪದ ಅಪರಾಧಗಳನ್ನೂ ತಿಳಿಸಲಾಗಿದೆ.

೯ನೇ ವಿಭಾಗದಲ್ಲಿ ಉಲ್ಲೇಖಿಸಲ್ಪಟ್ಟಿರುವ ಕಾನೂನಿನ ಉಲ್ಲಂಘನೆ ಪ್ರಕರಣಗಳಲ್ಲಿ ತೊಂದರೆಯಾದ ವ್ಯಕ್ತಿ ಅಪರಾಧಿಯಿಂದ ಒಂದು ಕೋಟಿ ರೂಪಾಯಿಯ ವರೆಗೂ ನಷ್ಟ ವನ್ನು ಕೇಳುವ ಅವಕಾಶವನ್ನು ಕೊಟ್ಟಿರುತ್ತದೆ. ಈ ರೀತಿಯ ಪ್ರಕರಣಗಳನ್ನು ಶ್ರೀಘ್ರ ಗತಿಯಲ್ಲಿ ವಿಚಾ ರಣೆ ನಡೆಸಿ ತೀರ್ಪು ಕೊಡಲು ‘‘ಆಡ್ಜುಡಿಕೇಶನ್’’ ವ್ಯವಸ್ಥೆ ಯನ್ನು ಒದಗಿಸಿಕೊಡಲಾಗಿದೆ.

ಮುಖ್ಯವಾಗಿ ಈ ವಿಭಾಗದಲ್ಲಿ ಉಲ್ಲೇಖವಾಗಿರುವ ಅಪರಾಧಗಳು ಸೆಕ್ಷನ್ ೪೩ ರಲ್ಲಿ ನಮೂದಿಸಲ್ಪಟ್ಟಿವೆ. ಇವುಗಳ ಸಾರಾಂಶ ಈ ರೀತಿ ಇದೆ.

‘‘ ಯಾವುದೇ ವ್ಯಕ್ತಿ ಯಾವುದೇ ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆಯ ಒಡೆಯನ ಅಥವಾ ಅಧಿಕಾರವನ್ನು ಹೊಂದಿರುವವನ ಅಪ್ಪಣೆಯಿಲ್ಲದೆ ಈ ಕೆಳಕಂಡ ಯಾವುದೇ ಕಾರ್ಯವನ್ನು ಮಾಡಿದರೆ ಅದರಿಂದ ಭಾಧಿತರಾದವರಿಗೆ ಒಂದು ಕೋಟಿ ರೂಪಾಯಿಯವರೆಗೆ ನಷ್ಟ ಪರಿಹಾರಕ್ಕೆ ಭಾಧ್ಯನಾಗುತ್ತಾನೆ.

೧. ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆಯ ಪ್ರವೇಶ ಪಡೆಯುವುದು.

೨. ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆ ಅಥವಾ ಮಾಹಿತಿ ಅಡಕ ವಸ್ತುಗಳಲ್ಲಿರುವ ಮಾಹಿತಿಯನ್ನು ತೆಗೆದುಕೊಳ್ಳುವುದೂ, ನಕಲು ಮಾಡಿಕೊಳ್ಳುವುದು.

೩. ಕಂಪ್ಯೂಟರ್, ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆ ಯೊಳಗೆ ರೋಗಾಣುಗಳನ್ನು ಸೇರಿಸುವುದು

೪. ಕಂಪ್ಯೂಟರ್, ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆ, ಅಥವಾ ಅದರಲ್ಲಿರುವ ಮಾಹಿತಿಗಾಗಲಿ, ತಂತ್ರಾಂಶಗಳಿಗಾಗಲೀ, ಕೆಡುಕುಂಟುಮಾಡುವುದು

೫. ಕಂಪ್ಯೂಟರ್, ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ಜಾಲವನ್ನು ವಿವಶಗೊಳ್ಳಿಸುವುದು

೬. ಯಾವುದೇ ವಿಧದಲ್ಲಿ ಕಂಪ್ಯೂಟರ್, ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ಜಾಲದ ಅಧಿಕೃತ ವ್ಯಕ್ತಿಗಳಿಗೆ ಪ್ರವೇಶ ತಡೆ ಒಡ್ಡುವುದು

೭. ಈ ಕಾನೂನಿನನ್ನು ಉಲ್ಲಂಘಿಸಿ ಯಾವುದೇ ವ್ಯಕ್ತಿಗೆ ಕಂಪ್ಯೂಟರ್, ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ಜಾಲದ ಪ್ರವೇಶ ಪಡೆಯಲು ಸಹಕರಿಸುವುದು.

೮. ಕಂಪ್ಯೂಟರ್, ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ಜಾಲದಲ್ಲಿ ಬದಲಾವಣೆಗಳನ್ನು ಮಾಡಿ ತಾನು ಪಡೆದ ಸೇವೆಗಳನ್ನು, ಬೇರೊಬ್ಬರ ಖಾತೆಗೆ ಹಾಕುವುದು.''

ಮಾತಂಕಾ ೨೦೦೦ ದ ೧೧ನೇ ವಿಭಾಗದಲ್ಲಿ ಉಲ್ಲೇಖವಾಗಿರುವ ಪ್ರಮುಖ ಅಪರಾಧಗಳ ಸಂಕ್ಷಿಪ್ತ ರೂಪ ಈ ಕೆಳಕಂಡಂತೆ ಇದೆ.

ಸೆಕ್ಷನ್ ೬೫: ಮಾಹಿತಿ ಬದಲಾವಣೆ

ಯಾವುದೇ ವ್ಯಕ್ತಿ ಪ್ರಜ್ಞಾ ಪೂರ್ವಕವಾಗಿ ಇಲ್ಲವೇ ಉದ್ದೇಶ ಪೂರ್ವಕವಾಗಿ, ಕಾನೂನಿನ ಪ್ರಕಾರ ಇಡಬೇಕಾದ ಕಂಪ್ಯೂಟರ್ ಮಾಹಿತಿಯನ್ನು ತಾನು ಅಥವಾ ತನ್ಮೂಲಕ ಬಚ್ಚಿಡುವುದೋ, ಕೆಡುಸುವುದೋ, ಬದಲಾಯಿಸುವುದೋ ಮಾಡಿದಲ್ಲಿ ಆ ವ್ಯಕ್ತಿಗೆ ೩ ವರ್ಷ ಸೆರೆವಾಸ, ಮತ್ತು ರೂಪಾಯಿ ೨ ಲಕ್ಷದ ವರೆಗೂ ದಂಡವನ್ನು ವಿಧಿಸಬಹುದು.

ಸೆಕ್ಷನ್ ೬೬: ಹ್ಯಾಕಿಂಗ್

ಯಾವುದೇ ವ್ಯಕ್ತಿ, ಯಾವುದೇ ವಿಧಾನದಿಂದ, ಉದ್ದೇಶ ಪೂರ್ವಕವಾಗಿ ಅಥವಾ ತಾನು ಬೇರಾರಿಗಾದರೂ ನಷ್ಟವನ್ನುಂಟು ಮಾಡುವ ಸಂಭವವಿದೆಯೆಂಬ ತಿಳುವಳಿಕೆಯಿದ್ದೂ, ಕಂಪ್ಯೂಟರ್‌ನ ಒಳಗಿರುವ ಮಾಹಿತಿಯನ್ನು ನಷ್ಟಗೊಳಿಸುವುದೋ, ಅಳಿಸುವುದೋ, ಪರಿವರ್ತಿಸುವುದೋ, ಅಥವಾ ಬೇರಾವುದೇ ರೀತಿಯಲ್ಲಿ ಅದರ ಬೆಲೆ ಅಥವಾ ಉಪಯುಕ್ತತೆ ಯನ್ನು ಕಡಿತಗಳಿಸುವುದೋ ಬಾಧೆಗೊಳಿಸುವುದೋ ಮಾಡಿದಲ್ಲಿ ಅದು ''ಹ್ಯಾಕಿಂಗ್'' ಎನಿಸುತ್ತದೆ. ಅಂತಹ ಅಪರಾಧಿಗೆ ೩ ವರ್ಷ ಸಜೆಯನ್ನೂ ಅಥವಾ ರೂ ೨ ಲಕ್ಷದ ವರೆಗೂ ದಂಡವನ್ನೂ ವಿಧಿಸಬಹುದು.

ಸೆಕ್ಷನ್ ೬೭: ಗಣಕ ಪತ್ರದ ಮೂಲಕ ಅಶ್ಲೀಲತೆ

ಯಾವುದೇ ವ್ಯಕ್ತಿ, ಅಶ್ಲೀಲ ವಿಷಯವನ್ನು ಅದರಿಂದ ಕೆಡುಕುಂಟಾಗ ಬಲ್ಲ ವ್ಯಕ್ತಿಗಳಿಗೆ ಗಣಕ ಪತ್ರದ ರೂಪದಲ್ಲಿ ಪ್ರಸಾರ ಮಾಡುವುದಾಗಲೀ, ಹಂಚುವುದಾಗಲೀ ಮಾಡಿದಲ್ಲಿ ಆ ವ್ಯಕ್ತಿಗೆ ಮೊದಲ ಅಪರಾಧದಲ್ಲಿ ೫ ವರ್ಷ ಸಜೆ ಹಾಗೂ ರೂಪಾಯಿ ೧ ಲಕ್ಷದ ವರೆಗೆ ದಂಡ ಹಾಗೂ ಎರಡನೇ ಬಾರಿ ಅಥವಾ ಮತ್ತೆ ನಡೆವ ಅಪರಾಧದಲ್ಲಿ ೧೦ ವರ್ಷ ಸಜೆ ಹಾಗೂ ರೂಪಾಯಿ ೨ ಲಕ್ಷದ ವರೆಗೆ ದಂಡ ವಿಧಿಸಬಹುದು.

ಸೆಕ್ಷನ್ ೭೦: ರಕ್ಷಿತ ವ್ಯವಸ್ಥೆ

ನಿಗದಿತ ಸರ್ಕಾರ ಗೆಜ಼ೆಟ್ ಸೂಚನೆಯಿಂದ ಯಾವುದೇ ಕಂಪ್ಯೂಟರ್, ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆ, ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ಜಾಲವನ್ನು ''ರಕ್ಷಿತ ವ್ಯವಸ್ಥೆ'' ಎಂದು ಘೋಷಿಸಿ ಅದರ ಅಧಿಕೃತ ಪ್ರವೇಶ ನಿಯಮಗಳನ್ನು ಬರವಣಿಗೆಯ ಮೂಲಕ ಪ್ರಕಟಮಾಡಿದ್ದರೆ, ಅಂತಹ ವ್ಯವಸ್ಥೆಯನ್ನು ಅತಿಕ್ರಮ ಪ್ರವೇಶ ಮಾಡಿದ ಅಥವಾ ಮಾಡಲು ಪ್ರಯತ್ನ ಪಟ್ಟ ವ್ಯಕ್ತಿಗೆ ೧೦ ವರ್ಷ ಸಜೆ ಮತ್ತು ದಂಡ ವಿಧಿಸಬಹುದು.

ಅಡ್ಜುಡಿಕೇಶನ್

ಅಡ್ಜುಡಿಕೇಶನ್ ಎಂಬುದು ಮಾತಂಕ ೨೦೦೦ ದ ೯ ನೇ ವಿಭಾಗದ (ಸಿವಿಲ್ ರೂಪದ) ಅಪರಾಧಗಳಿಗೆ ಅನ್ವಯವಾಗುವ ಪರ್ಯಾಯ ನ್ಯಾಯಾಂಗ ವ್ಯವಸ್ಥೆ.

ಇದರ ಪ್ರಕಾರ ನೊಂದಿರುವ ವ್ಯಕ್ತಿ ನಿರ್ಧಿಷ್ಟ ಅಡ್ಜುಡಿಕೇಟರ್‌ಗೆ ಅಹವಾಲನ್ನು ಸಲ್ಲಿಸಬಹುದು. ಈ ಅರ್ಜಿಯಲ್ಲಿ ಅಪರಾಧದ ವಿವರ (ತನಗೆ ತಿಳಿದಷ್ಟು),

ಆರೋಪಿಯ ವಿವರ (ತನಗೆ ತಿಳಿದಂತೆ), ಅಪರಾಧ ನಡೆದ ಸ್ಥಳ, ದಿನಾಂಕ, ಸಮಯ, ತನಗಾದ ನಷ್ಟ ಮುಂತಾದ ವಿವರವನ್ನು ಸಲ್ಲಿಸಬೇಕು. ಅರ್ಜಿಯೊಡನೆ ತಾನು ಕೇಳುವ ನಷ್ಟ ಪರಿಹಾರ ದ ಶೇಖಡಾ ೧೦ ರ ಷ್ಟು ಶುಲ್ಕವನ್ನು ಸಲ್ಲಿಸಬೇಕು.

ಈ ವ್ಯವಸ್ಥೆಯಲ್ಲಿ, ಅಡ್ಜುಡಿಕೇಟರ್ ಅಥವಾ ವಿಚಾರಣಾಧಿಕಾರಿ ಆರೋಪಿಗೆ ನೋಟೀಸ್ ಜಾರಿ ಮಾಡಿ ಅವನ ಸಮಕ್ಷಮ ಇಲ್ಲವೇ ಗೈರು ಹಾಜರಿಯಲ್ಲಿ ವಿಚಾರಣೆ ನಡೆಸಿ ತೀರ್ಪು ಕೊಡಬಹುದು. ಅಪರಾಧದ ಬಗ್ಗೆ ಹೆಚ್ಚಿನ ತನಿಖೆ ನಡೆಯಬೇಕಾಗಿದ್ದಲ್ಲಿ ವಿಚಾರಣಾಧಿಕಾರಿ ತನ್ನ ವ್ಯಾಪ್ತಿಯಲ್ಲಿ ಬರುವ ಪೋಲೀಸ್ ಅಧಿಕಾರಿಗಳ ಸಹಾಯ ಪಡೆಯಬಹುದು.

ಕೇಂದ್ರ ಸರ್ಕಾರದ ಸೂಚನೆಯಂತೆ ಸಾಮಾನ್ಯವಾಗಿ ಈ ರೀತಿಯ ವಿಚಾರಣೆ ೪ ತಿಂಗಳಲ್ಲಿ ಮುಗಿಯಬೇಕು. ವಿಶೇಷ ಕಾರಣಗಳಿದ್ದಲ್ಲಿ ೨ ತಿಂಗಳು ಹೆಚ್ಚಿನ ಕಾಲ ತೆಗೆದುಕೊಳ್ಳಬಹುದು.

ಮಾರ್ಚ್ ೨೫, ೨೦೦೩ ರಂದು ಹೊರಪಡಿಸಲಾದ ಕೇಂದ್ರ ಸರ್ಕಾರದ ಸೂಚನೆಯ ಪ್ರಕಾರ ಪ್ರತಿ ರಾಜ್ಯ ಸರ್ಕಾರದ "ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ನಿರ್ದೇಶಕ" ರನ್ನು (Secretary-Information Technology) ಆ ರಾಜ್ಯದ "ಅಡ್ಜುಡಿಕೇಟರ್" ಎಂದು ನೇಮಕ ಮಾಡಲಾಗಿದೆ.

ಕರ್ನಾಟಕದಲ್ಲಿ ಈಗ ಯಾವುದೇ ಅಡ್ಜುಡಿಕೇಶನ್ ಅರ್ಜಿ ಇದ್ದಲ್ಲಿ ಅದನ್ನು ಕರ್ನಾಟಕ ಸರ್ಕಾರದ ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ನಿರ್ದೇಶಕರಿಗೆ ಕಳುಹಿಸಬಹುದು. ಮಾತಂಕಾ ದ ೯ನೇ ವಿಭಾಗದ ಯಾವುದೇ ಅಪರಾಧದಲ್ಲಿ ಕರ್ನಾಟಕದ ಗಡಿಯೊಳಗಿನ ಕಂಪ್ಯೂಟರ್ ಭಾಗಿಯಾಗಿದ್ದರೆ ಅದು ಕರ್ನಾಟಕದ ಅಡ್ಜುಡಿಕೇಟರ್ ನ ವ್ಯಾಪ್ತಿಯಲ್ಲಿ ಬರುತ್ತದೆ.

ಆಡ್ಜುಡಿಕೇಶನ್ ನಲ್ಲಿ ಹೊರಬಂದ ತೀರ್ಪಿನ ಬಗ್ಗೆ ದಾವೆದಾರರಲ್ಲಿ ತೃಪ್ತಿ ದೊರಕದೆ ಹೋದಲ್ಲಿ ಅವರು ಸೈಬರ್ ಅಪಲೇಟ್ ಟ್ರೈಬ್ಯುನಲ್ ಗೆ ಅಪೀಲ್ ಹೋಗಲು ಅವಕಾಶವಿದೆ. ನಂತರದ ಅಪೀಲನ್ನು ಹೈಕೋರ್ಟ್ ಗೆ ಮಾಡಬಹುದು.

ಇದುವರೆಗೂ ಸೈಬರ್ ಅಪಲೇಟ್ ಟ್ರೈಬ್ಯುನಲ್ ಸ್ಥಾಪನೆಯಾಗಿಲ್ಲವಾದ್ದರಿಂದ ಅಡ್ಜುಡಿಕೇಟರ್ ನ ತೀರ್ಪಿನ ಮೇಲಿನ ಅಪೀಲನ್ನು ಈಗ ಹೈಕೋರ್ಟಿಗೆ ಮಾಡಬಹುದೆಂಬ ಅಭಿಪ್ರಾಯ ಇದೆ.

ಭಾರತದಲ್ಲಿ ಸಿವಿಲ್ ಪ್ರಕರಣಗಳು ಹಲವಾರು ವರ್ಷ ನ್ಯಾಯಾಲಯದಲ್ಲಿ ಕೊಳೆಯುವುದು ಸರ್ವೇ ಸಾಮಾನ್ಯ. ಹಾಗಿದ್ದೂ ಅಡ್ಜುಡಿಕೇಶನ್ ೪ ತಿಂಗಳೊಳಗೆ ತೀರ್ಮಾನ ವಾಗುವ ಸಾಧ್ಯತೆ ಇರುವುದು ಜನ ಸಾಮಾನ್ಯರಿಗೆ ವರ ಪ್ರಸಾದ ವೆನ್ನಬಹುದು.

ಜನರು ಈ ವಿಷಯದಲ್ಲಿ ನೆನಪಿನಲ್ಲಿಡಬೇಕಾದ ಅಂಶವೆಂದರೆ, ಯಾವುದೇ ಪ್ರಕರಣದಲ್ಲಿ ದೂರು ಬೇಜವಾಬ್ದಾರಿಯಿಂದ ಮಾಡಿದ್ದೆಂದು ಅಡ್ಜುಡಿಕೇಟರ್ ಭಾವಿಸಿದಲ್ಲಿ, ದೂರು ಕೊಟ್ಟವರಿಗೆ ರೂಪಾಯಿ ೨೫೦೦೦ ದ ವರೆಗೆ ತಪ್ಪು ದಂಡ ವಿಧಿಸಲು ಅವಕಾಶವಿರುತ್ತದೆ.

ಮಾತಂಕಾ ೨೦೦೦ ದಲ್ಲಿ ಪ್ರಸ್ತಾಪಿಸಿರುವ ಅಡ್ಜುಡಿಕೇಶನ್ ವ್ಯವಸ್ಥೆ ನಮ್ಮ ದೇಶದ ನ್ಯಾಯಾಂಗ ವ್ಯವಸ್ಥೆಯ ಒಂದು ಹೊಸ ಆಯಾಮವೆಂದರೆ ತಪ್ಪಿಲ್ಲ.

ಮಧ್ಯವರ್ತಿ ಸಂಸ್ಥೆ ಗಳು

ಅಂತರ್ಜಾಲ ವ್ಯವಹಾರ ಗಳಲ್ಲಿ ಮಧ್ಯವರ್ತಿ ಸಂಸ್ಥೆಗಳ ಪಾತ್ರ ಬಹಳ ಮುಖ್ಯ.

ಮೊತ್ತ ಮೊದಲಿಗೆ ಯಾವುದೇ ವ್ಯಕ್ತಿ ಅಂತರ್ಜಾಲ ಪ್ರವೇಶಿಸಬೇಕಾದರೆ ಈ ಸೇವೆಯನ್ನು ಒದಗಿಸುವ ಐ.ಎಸ್.ಪಿ. (ಇಂಟರ್ನೆಟ್ ಸರ್ವಿಸ್ ಪ್ರೊವೈಡರ್ ಅಥವಾ ಅಂತರ್ಜಾಲ ಸೇವಾದಾರ) ಅಗತ್ಯ. ಉದಾಹರಣೆಗೆ ವಿ.ಎಸ್.ಎನ್.ಎಲ್., ಸಿಫ್ಲಿ, ಮಂತ್ರ ಆನ್ ಲೈನ್, ಬಿ.ಎಸ್.ಎನ್.ಎಲ್. ಮತ್ತಿತರ ಸಂಸ್ಥೆಗಳು.

ನಂತರ ಅಂತರ್ಜಾಲದಲ್ಲಿ ಇ–ಮೈಲ್ ಮುಂತಾದ ಸೇವೆಯನ್ನು ಕೊಡುವ ಸಂಸ್ಥೆಗಳು ಅಪರಾಧಗಳಲ್ಲಿ ಮುಖ್ಯ ಪಾತ್ರವನ್ನು ವಹಿಸುತ್ತವೆ.
ಇದಲ್ಲದೆ ಕಂಪ್ಯೂಟರ್ ಇಲ್ಲದವರಿಗೂ ಅಂತರ್ಜಾಲಕ್ಕೆ ಪ್ರವೇಶ ಮಾಡುವುದಕ್ಕೆ ಸಹಕಾರ ಮಾಡುವ ವ್ಯವಸ್ಥೆ ಸೈಬರ್ ಕೆಫೆಗಳದ್ದು.

ಸೈಬರ್ ಕೆಫೆ ಗಳಂತೆಯೇ ಕಂಪನಿಗಳು, ವಿದ್ಯಾ ಸಂಸ್ಥೆಗಳೂ ಮತ್ತು ಸರ್ಕಾರಿ ಶಾಖೆಗಳೂ ಕೂಡ ಕಂಪ್ಯೂಟರ್ ಜಾಲಗಳನ್ನು ಹೊಂದಿದ್ದು ವಿವಿಧ ವ್ಯಕ್ತಿಗಳು ಈ ಜಾಲದ ಮೂಲಕ ಅಂತರ್ಜಾಲಕ್ಕೆ ಪ್ರವೇಶ ಪಡೆಯುತ್ತಾರೆ.

ಯಾವುದೇ ಅಂತರ್ಜಾಲ ಅಪರಾಧ ನಡೆದಾಗ ಈ ವಿವಿಧ ಮಧ್ಯವರ್ತಿಗಳು ಅಪರಾಧಕ್ಕೆ ಸಹಕರಿಸಿದ ವ್ಯಕ್ತಿಗಳಾಗುತ್ತಾರೆ. ಇದರಿಂದ ಅಪರಾಧದ ಜವಾಬ್ದಾರಿ ಸ್ವಲ್ಪ ಮಟ್ಟಿಗೆ ಅವರುಗಳ ಮೇಲೆ ಕೂಡ ಬೀಳುತ್ತದೆ.

ಈ ವಿಷಯವನ್ನು ಗಮನದಲ್ಲಿಟ್ಟುಕೊಂಡು ಮಾತಂಕಾ ೨೦೦೦ ದಲ್ಲಿ ಈ ಮಧ್ಯವರ್ತಿಗಳಿಗೆ ಸೆಕ್ಷನ್ ೭೯ ರ ಮೂಲಕ ರಕ್ಷಣೆ ಒದಗಿಸಲಾಗಿದೆ.

ಆಂತರ್ಜಾಲದ ಸದುಪಯೋಗವಾಗಬೇಕಿದ್ದಲ್ಲಿ ಈ ಮಧ್ಯವರ್ತಿಗಳು ಅನಗತ್ಯವಾಗಿ ಅಪರಾಧದ ವಿಚಾರಣೆಗಳಲ್ಲಿ ಸಿಲುಕಿ ತೊಂದರೆಗೊಳ್ಳುವುದು ತಪ್ಪಬೇಕು ಎಂಬುದು ಈ ಸೆಕ್ಷನ್ ಉದ್ದೇಶವೆನ್ನಬಹುದು.

ಸೆಕ್ಷನ್ ೭೯ ರ ಉಲ್ಲೇಖ ಈ ಕೆಳಕಂಡಂತೆ ಇದೆ.

ಜಾಲ ಸೇವಾದಾರರು ಕೆಲವು ಸಂದರ್ಭಗಳಲ್ಲಿ ಹೊಣೆಯಾಗುವುದಿಲ್ಲ:

ಸಂಶಯ ನಿವಾರಣಾ ಪ್ರಯುಕ್ತ ಈ ಮೂಲಕ ಘೋಷಿಸುವುದೇನೆಂದರೆ, ಜಾಲ ಸೇವಾದಾರನಾಗಿ ಸೇವೆ ಸಲ್ಲಿಸುತ್ತಿರುವ ಯಾವುದೇ ವ್ಯಕ್ತಿ, ಯಾವುದೇ ಅಪರಾಧ ಅಥವಾ ಉಲ್ಲಂಘನೆ ತನ್ನ ಅರಿವಿಲ್ಲದೆ ಮತ್ತು ತಾನು ಉಚಿತ ಪರಿಶ್ರಮ ವಹಿಸಿದ್ದರೂ ಕೂಡ ನಡೆದಿದೆ ಎಂದು ಪ್ರಮಾಣ ಮಾಡಲು ಯಶಸ್ವಿಯಾದಲ್ಲಿ, ಅವನು ತನ್ನದಲ್ಲದ ಮಾಹಿತಿಯನ್ನು ಒದಗಿಸಿದ್ದಕ್ಕಾಗಿ ಈ ಕಾಯಿದೆ, ಅಥವಾ ಅದರಡಿಯಲ್ಲಿ ಮಾಡುವ ನಿಯಮಗಳು ಮತ್ತು ಸೂಚನೆಗಳ ಪ್ರಕಾರ ಹೊಣೆಯಾಗುವುದಿಲ್ಲ.

ವಿಷದೀಕರಣ: ಈ ಸೆಕ್ಷನ್‌ನ ಉದ್ದೇಶಕ್ಕಾಗಿ ಯಾವ ವ್ಯಕ್ತಿ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಸಂದೇಶವನ್ನು ಇನ್ನೊಬ್ಬರ ಪರವಾಗಿ ಪಡೆಯುವುದು, ಸಂಗ್ರಹಿಸಿಡುವುದು, ಕಳುಹಿಸುವುದು ಅಥವಾ ಆ ಸಂದೇಶದ ಬಗ್ಗೆ ಯಾವುದೇ ಸೇವೆಯನ್ನು ಸಲ್ಲಿಸುವುದನ್ನು ಮಾಡುತ್ತಾನೋ ಅವನನ್ನು ''ಜಾಲ ಸೇವಾದರ''ಎಂದು ಪರಿಗಣಿಸಲಾಗುತ್ತದೆ.

ಈ ಸೆಕ್ಷನ್ ಮುಖ್ಯವಾಗಿ ಯಾಹೂ ಮತ್ತು ಹಾಟ್ ಮೈಲ್ ಮುಂತಾದ ಇ–ಮೈಲ್ ಸೇವಾದಾರರಿಗೆ ಅನ್ವಯಿಸುವಂತೆ ಕಂಡರೂ ''.. ಸಂದೇಶದ ಬಗ್ಗೆ ಯಾವುದೇ ಸೇವೆ..'' ಎಂದು ಸೂಚಿಸಿರುವುದನ್ನು ತೆಗೆದು ಕೊಂಡರೆ ಇ–ಮೈಲ್ ಸೇವೆಯನ್ನು

ಪ್ರವೇಶಮಾಡಲು ಬೇಕಾದ ಅಂತರ್ಜಾಲ ಸೇವೆ (ಐ.ಎಸ್.ಪಿ), ಕಂಪ್ಯೂಟರ್ ಇಲ್ಲದವರೂ ಇ–ಮೈಲ್ ಸೇವೆಯನ್ನು ಉಪಯೋಗಿಸಲು ಅನುವು ಮಾಡಿಕೊಡುವ ಸೈಬರ್ ಕೆಫೆ ಸೇವೆ, ಕೆಲಸಗಾರರು ಅಥವಾ ವಿದ್ಯಾರ್ಥಿಗಳು ಇ–ಮೈಲ್ ಬಳಸಲು ಅನುವು ಮಾಡಿಕೊಡುವ ಕಂಪನಿ ಅಥವಾ ವಿದ್ಯಾಸಂಸ್ಥೆಯ ಜಾಲ ನಿರ್ವಹಣೆ ಕೂಡ ಈ ಸೆಕ್ಷನ್ ಒಳಗೆ ನಾವು ತರಬಹುದು.

ಅಂತೆಯೇ ಅಂತರ್ಜಾಲದಲ್ಲಿ ಎಲ್ಲಾ ವ್ಯವಹಾರಗಳೂ ಕಂಪ್ಯೂಟರ್ ನಿಂದ ಕಂಪ್ಯೂಟರ್ ಗೆ ಹರಿಯುವುದು, ಸಂದೇಶದ ತುಣುಕುಗಳ (ಇನ್ಫರ್‌ಮೇಶನ್ ಪ್ಯಾಕೆಟ್) ರೂಪದಲ್ಲಿ ಮತ್ತು ಸಂದೇಶ ವಾಹಕ ಭಾಶೆಯಲ್ಲಿ (TCP/IP Protocol). ಆದ್ದರಿಂದ ಮಾತಂಕಾ–೨೦೦೦ ದ ಸೆಕ್ಷನ್ ೭೯ ಅನ್ನು ಎಲ್ಲಾ ಅಂತರ್ಜಾಲ ಸೇವಾ ದಾರರಿಗೂ ಅನ್ವಯಗೊಳಿಸಬಹುದು.

ಈ ಸೆಕ್ಷನ್ ನಲ್ಲಿ ಮುಖ್ಯವಾಗಿ ನಾವು ಗಮನಿಸಬೇಕಾದ ಅಂಶವೆಂದರೆ, ಇದರ ಪ್ರಕಾರ ಎಲ್ಲಾ ಜಾಲ ಮುಖ್ಯಸ್ಥರೂ "ಉಚಿತ ಪರಿಶ್ರಮ" (Due-Diligence) ವಹಿಸದಿದ್ದರೆ ಅವರು ಜಾಲದಲ್ಲಿ ನಡೆಯುವ ಅಪರಾಧಗಳಿಗೆ ಹೊಣೆ ಹೊರಬೇಕಾಗಬಹುದು. ಯಾವ ಪರಿಶ್ರಮ "ಉಚಿತ" ಎನ್ನುವುದು ಚರ್ಚಾಸ್ಪದ ವಿಷಯ. ಮುಖ್ಯವಾಗಿ ಇದು ಸಂದರ್ಭಕ್ಕೆ ಅನುಗುಣವಾಗಿ ಯಾವ ಎಚ್ಚರಿಕೆಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳಲು ಸಾಧ್ಯ ಮತ್ತು ಅಗತ್ಯ ಎಂಬ ಬಗ್ಗೆ ನಿಪುಣರ ಅಭಿಪ್ರಾಯವನ್ನು ಅವಲಂಬಿಸಿರುತ್ತದೆ.

ಪೋಲೀಸರ ಅಧಿಕಾರ

ಮಾತಂಕಾ–೨೦೦೦ ಅಂತರ್ಜಾಲದ ಅಪರಾಧಗಳ ಬಗ್ಗೆ ವಿಚಾರ ಮಾಡಿರುವಂತೆ, ಅಪರಾಧಗಳ ಶೋಧನೆ, ವಿಚಾರಣಾ ವಿಧಾನ ಮುಂತಾದ ವಿಶಯಗಳ ಬಗ್ಗೆಯೂ ಕೆಲವು ವಿಷೇಶ ನಿಯಮಗಳನ್ನು ತಿಳಿಸಲಾಗಿದೆ.

ಸೆಕ್ಷನ್ ೭೮ ರ ಪ್ರಕಾರ ಕ್ರಿಮಿನಲ್ ಪ್ರೊಸೀಜರ್ ಕೋಡ್ ನಲ್ಲಿರುವ ಸಂಹಿತೆ ಏನಿದ್ದರೂ ಮಾತಂಕಾ ದ ಕಾಯಿದೆಯಲ್ಲಿನ ಯಾವುದೇ ಶೋಧನಾ ಕಾರ್ಯವನ್ನು ಡಿ.ಎಸ್.ಪಿ. ಶ್ರೇಯಾಂಕದ ಕೆಳಮಟ್ಟದ ಅಧಿಕಾರಿ ಮಾಡುವಂತಿಲ್ಲ.

ಹಾಗೆಯೇ, ಸೆಕ್ಷನ್ ೮೦ ರ ಪ್ರಕಾರ, ಸಾರ್ವಜನಿಕ ಸ್ಥಳಗಳಲ್ಲದೆ ಬೇರೆಲ್ಲೂ ವಾರಂಟ್ ಇಲ್ಲದೆ ಶೋಧನೆ ನಡೆಸುವುದಾಗಲೀ, ಅಥವಾ ಬಂಧಿಸುವುದಾಗಲೀ ಯಾರಾದರೂ ಮಾಡುವಂತಿಲ್ಲ. ಸಾರ್ವಜನಿಕ ಸ್ಥಳಗಳಲ್ಲಿ ಮಾತ್ರ, ಡಿ.ಎಸ್.ಪಿ. ಶ್ರೇಯಾಂಕಕ್ಕೆ ಕಡಿಮೆಯಿಲ್ಲದ ಪೋಲೀಸ್ ಅಧಿಕಾರಿಗಳು ಅಥವಾ ರಾಜ್ಯ ಇಲ್ಲವೇ ಕೇಂದ್ರ ಸರ್ಕಾರದಿಂದ ನಿಯಮಿತವಾದ ಅಧಿಕಾರಿಗಳು, ಯಾವುದಾದರೂ ಅಪರಾಧ ನಡೆಯುತ್ತಿದರೆ, ಅಥವಾ ಅವರ ದೃಷ್ಟಿಯಲ್ಲಿ ನಡೆಯುವ ಸಂಭವ ಕಂಡು ಬಂದರೆ ಅಪರಾಧಿಯನ್ನು ವಾರಂಟ್ ಇಲ್ಲದೆ ಬಂಧಿಸಬಹುದು ಮತ್ತು ಸ್ಥಳದಲ್ಲಿ ಶೋಧನೆ ನಡೆಸಬಹುದು.

ಈ ಸೆಕ್ಷನ್ ಉದ್ದೇಶಕ್ಕೆ ''ಸಾರ್ವಜನಿಕ ಸ್ಥಳ'' ಎಂದರೆ, ಸಾರ್ವಜನಿಕ ಸಾರಿಗೆ ವ್ಯವಸ್ಥೆ, ಹೋಟೆಲ್, ಅಂಗಡಿ, ಅಥವಾ ಬೇರಾವುದೇ ಸಾರ್ವಜನಿಕರು ಬಂದು ಹೋಗುವ ಸ್ಥಳ ಸೇರುತ್ತವೆ.

ಆಂತಹ ಸಂಧರ್ಭಗಳಲ್ಲಿ ಭಂಧಿಸಿದ ವ್ಯಕ್ತಿಯನ್ನು ಆದಷ್ಟು ಬೇಗ ಮ್ಯಾಜಿಸ್ಟ್ರೇಟ್ ಮುಂದೆ ಹಾಜರು ಪಡಿಸಿ ಮುಂದಿನ ಕ್ರಮ ಜರುಗಿಸ ಬಹುದು.

ಇಲ್ಲಿ ಹೇಳದೇ ಇರುವ ವಿಷಯಗಳಲ್ಲಿ ಕ್ರಿಮಿನಲ್ ಪ್ರೊಸೀಜರ್ ಕೋಡ್ ಅನ್ವಯವಾಗುತ್ತದೆ.

ಇತರ ವಿಷಯಗಳು

ಇನ್ನಿತರ ಮುಖ್ಯ ಅಂಶಗಳ ಸಂಕ್ಷಿಪ್ತ ವಿವರಣೆ ಕೆಳಕಂಡಂತೆ ಇದೆ.

ಸೆಕ್ಷನ್ ೧೧ ರ ಪ್ರಕಾರ ಯಾವುದೇ ಸಂದೇಶದ ಭಾದ್ಯತೆ ಅದನ್ನು ಕಳುಹಿಸಿದ ವ್ಯಕ್ತಿಗೆ ಸೇರಿರುತ್ತದೆ. ಸಂದೇಶ ಯಾವುದಾದರೂ ಕಂಪ್ಯೂಟರ್ ನಿಂದ ಹೊರಹೊಮ್ಮಿದ್ದರೆ ಅದರ ಮಾಲೀಕ ಅಥವಾ ಅದನ್ನು ಕಳುಹಿಸುವಂತೆ ತಂತ್ರಾಂಶವನ್ನು ರೂಢಿಸಿದವನು ಆ ಸಂದೇಶದ ಭಾದ್ಯತೆಯನ್ನು ಹೊರಬೇಕಾಗುತ್ತದೆ.

ಸೆಕ್ಷನ್ ೧೩ ರಲ್ಲಿ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಸಂದೇಶದ ಸ್ಥಳ ಮತ್ತು ಸಮಯ ನಿರ್ಧಾರ ಮಾಡುವ ವಿಧಾನ ಹೇಳಲ್ಪಟ್ಟಿದೆ.

ಇದರ ಪ್ರಕಾರ ಬೇರೆ ಒಪ್ಪಂದವಿಲ್ಲದಿದ್ದರೆ, ಸಂದೇಶ ಎಲ್ಲಿಂದ ಕಳುಹಿಸಲ್ಪಟ್ಟಿದ್ದರೂ ಸಹ ಸಂದೇಶವನ್ನು ಕಳುಹಿಸುವವರ ಸಾಮಾನ್ಯ ವಾಸ ಸ್ಥಳ ಅಥವಾ ಸಂದೇಶ ಕಳುಹಿಸುವ ವ್ಯಕ್ತಿ ಕಂಪನಿಯಾಗಿದ್ದರೆ, ಅದರ ಮುಖ್ಯ ಕಛೇರಿ ಇರುವ ಸ್ಥಳ, ಆ ವ್ಯಕ್ತಿ ಕಳುಹಿಸುವ ಸಂದೇಶದ ಮೂಲ ಸ್ಥಳವೆಂದು ನಿರ್ಧರಿಸಲ್ಪಡುತ್ತದೆ.

ಸಂದೇಶ ಕಳುಹಿಸುವವರ ಕಂಪ್ಯೂಟರ್ ನಿಂದ ಹೊರಗೆ ಹೋಗುವ ಸಮಯ ಕಳುಹಿಸುವ ಸಮಯವೆಂದು ನಿರ್ಧರಿಸಲ್ಪಡುತ್ತದೆ.

ಸಂದೇಶ ಪಡೆಯುವವರು ಮುಂಚೆಯೇ ತಿಳಿಸಿದ ಇ–ಮೈಲ್ ವಿಳಾಸಕ್ಕೆ ಸಂದೇಶ ಕಳುಹಿಸಲ್ಪಟ್ಟಿದ್ದರೆ, ಅದು ಅವರು ಸಂದೇಶವನ್ನು ಯಾವಾಗ ಗಮನಿಸಿದರೂ ಅವರ ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆಯೊಳಗೆ ಪ್ರವೇಶ ಮಾಡಿದ ಸಮಯ ಸಂದೇಶವನ್ನು ಪಡೆದ ಸಮಯವೆಂದು ನಿರ್ಧರಿಸಲ್ಪಡುತ್ತದೆ.

ಒಂದು ವೇಳೆ ಸಂದೇಶವನ್ನು ವಿಳಾಸದಾರರು ನಿಗದಿಪಡಿಸಿದ ವಿಳಾಸಕ್ಕೆ ಕಳುಹಿಸದೆ ಅವರದೇ ಬೇರೆ ವಿಳಾಸಕ್ಕೆ ಕಳುಹಿಸಲ್ಪಟ್ಟಿದ್ದರೆ ಅದನ್ನು ಅವರು ತೆರೆದ ಸಮಯವನ್ನು ಸಂದೇಶ ತಲುಪಿದ ಸಮಯವೆಂದು ತಿಳಿಯಲಾಗುತ್ತದೆ.

ಸೆಕ್ಷನ್ ೮೧ ರ ಪ್ರಕಾರ ಯಾವುದೇ ವಿಷಯ ಮಾತಂಕಾ ೨೦೦೦ ಕಾಯಿದೆಯಲ್ಲಿ ಉಲ್ಲೇಖವಾಗಿದ್ದಲ್ಲಿ ಅದರ ಬಗ್ಗೆ ಬೇರೆ ಕಾಯಿದೆಗಳಲ್ಲಿರುವ ಉಲ್ಲೇಖಗಳು ಪರಿಗಣನೆಗೆ ಬರುವುದಿಲ್ಲ.

ಮಾತಂಕಾ ೨೦೦೦ ದೊಡನೆ, ಮುಂಚಿನ ಕೆಲವು ಕಾಯಿದೆಗಳಲ್ಲಿ ಸಾಂದರ್ಭಿಕ ಬದಲಾವಣೆಗಳಾಗಿವೆ. ಇಂಡಿಯನ್ ಪೀನಲ್ ಕೋಡ್, ಇಂಡಿಯನ್ ಎವಿಡೆನ್ಸ್ ಆ್ಯಕ್ಟ್ ನಲ್ಲಿನ ಬದಲಾವಣೆಗಳು ಇದರಲ್ಲಿ ಮುಖ್ಯವಾಗಿದೆ.

ಈ ಬದಲಾವಣೆಗಳಲ್ಲಿ ಮುಖ್ಯವಾಗಿ ಗಮನದಲ್ಲಿಡಬೇಕಾದ ವಿಷಯ ಇಂಡಿಯನ್ ಎವಿಡೆನ್ಸ್ ಆ್ಯಕ್ಟ್ ನ ಸೆಕ್ಷನ್ ೬೫ ಬಿ. ಇದರ ಪ್ರಕಾರ ಯಾವುದೇ ಗಣಕ ಪತ್ರವನ್ನು, ನಿಗದಿತ ಪ್ರಮಾಣಗಳೊಂದಿಗೆ, ಮುದ್ರಣ ರೂಪದಲ್ಲಿ ನ್ಯಾಯಾಲಯದಲ್ಲಿ ಪ್ರಸ್ತುತ ಪಡಿಸಬಹುದು. ಇದು ಎಲ್ಲಾ ಅಪರಾಧ ಸಂಧರ್ಭಗಳಲ್ಲೂ ಉಪಯೋಗಕ್ಕೆ ಬರುವ ವಿಚಾರ.

(ಮಾತಂಕಾ ೨೦೦೦ ದ ಬಗ್ಗೆ ಹೆಚ್ಚಿನ ವಿವರಗಳಿಗೆ http://www.naavi.org ವೆಬ್ ಸೈಟ್ ನೋಡಿ)

ಅಧ್ಯಾಯ ೬ ಸೈಬರ್ ಕೆಫೆ ನಿಯಂತ್ರಣ

ಅಂತರ್ಜಾಲದ ಉಪಯೋಗಗಳನ್ನು ಸಾಮಾನ್ಯ ಜನಸಮುದಾಯಕ್ಕೆ ತಲುಪಿಸುವುದರಲ್ಲಿ ಸೈಬರ್ ಕೆಫೆ ಗಳಿಗೆ ಮಹತ್ತರದ ಪಾತ್ರ ಇದೆ. ಕಂಪ್ಯೂಟರ್ ಬೆಲೆ ಕಡಿಮೆಯಾಗಿ ಬರುತ್ತಿದ್ದರೂ, ಇತ್ತೀಚಿನ ದಿನಗಳಲ್ಲಿ ತಂತ್ರಾಂಶದ ಬೆಲೆ ಹೆಚ್ಚುತ್ತಿರುವುದೇ ಅಲ್ಲದೆ, ರೋಗಾಣು ನಿರೋಧಕ, ಹ್ಯಾಕಿಂಗ್ ನಿರೋಧಕ, ಸ್ಪ್ಯಾಮ್ ನಿರೋಧಕ ಮುಂತಾದ ಉಪ ತಂತ್ರಾಂಶಗಳ ಅವಶ್ಯಕತೆಗಳು ಹೆಚ್ಚುತ್ತಿವೆ. ಅಲ್ಲದೆ, ಟೆಲಿಫೋನ್ ಮೂಲಕ ಅಂತರ್ಜಾಲ ಸೇವೆಯನ್ನು ಪಡೆಯಬೇಕಾದರೆ ಘಂಟೆಗೆ ೩೦ ರೂಪಾಯಿಗೂ ಹೆಚ್ಚು ಖರ್ಚು ಮಾಡಬೇಕಾಗಿರುತ್ತದೆ, ಇದೆಲ್ಲಾ ಕಾರಣದಿಂದ ಜನ ಸಾಮಾನ್ಯರಿಗೆ ಅಂತರ್ಜಾಲ ಇನ್ನೂ ದುಬಾರಿ ಸೇವೆಯಾಗಿಯೇ ಉಳಿದಿದೆ. ಈ ಪರಿಸರದಲ್ಲಿ ಯಾವ ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ತಂತ್ರಾಂಶದ ಖರ್ಚಿಲ್ಲದೆ, ಟೆಲಿಫೋನ್ ಅಥವಾ ಅಂತರ್ಜಾಲ ಸೇವಾ ಖರ್ಚಿಲ್ಲದೆ ಘಂಟೆಗೆ ೧೦-೧೫ ರೂಪಾಯಿಗೂ ಅಂತರ್ಜಾಲ ಸೇವೆ ನಮ್ಮ ಕೈಗೆಟಕುವಂತೆ ಮಾಡಿರುವುದು ಸೈಬರ್ ಕೆಫೆಗಳು.

ಈ ಸೈಬರ್ ಕೆಫೆಗಳಲ್ಲಿ ಕೆಲವು ಅಶ್ಲೀಲತೆಯ ಪ್ರಚಾರದಿಂದ ಹಣ ಮಾಡುತ್ತಿರುವುದರಿಂದ ಸೈಬರ್ ಕೆಫೆಗಳಿಗೆಲ್ಲಾ ಕೆಟ್ಟ ಹೆಸರು ಬಂದು ಬಿಟ್ಟಿದೆ. ಇದಲ್ಲದೆ ಸಾಮಾನ್ಯವಾಗಿಯೇ ಸೈಬರ್ ಅಪರಾಧಗಳನ್ನು ಮಾಡುವ ಅನೇಕರು ಸೈಬರ್ ಕೆಫೆಗಳನ್ನು ಉಪಯೋಗಿಸುವುದು ಸಹಜ. ಇದೆಲ್ಲಾ ಕಾರಣಗಳಿಂದ ಸೈಬರ್ ಕೆಫೆಗಳ ಮೇಲೆ ನಿಯಂತ್ರಣ ತರಬೇಕೆಂದು ಕೆಲವು ರಾಜ್ಯಗಳಲ್ಲಿ ಕ್ರಮಗಳನ್ನು ಕೈಗೊಳ್ಳಲಾಗಿದೆ.

ಈ ಸಂದರ್ಭದಲ್ಲಿ ನಾವು ನೆನಪಿನಲ್ಲಿಡಬೇಕಾದ ಅಂಶವೆಂದರೆ, ಸೈಬರ್ ಕೆಫೆ ಎಂಬುದು ಅಂತರ್ಜಾಲ ಮಾಧ್ಯಮವನ್ನು ಜನ ಸಾಮಾನ್ಯರು

ಉಪಯೋಗಿಸುವುದಕ್ಕೆ ಇರುವ ಸಾಧನ ಮಾತ್ರ. ಇದನ್ನು ಉಪಯೋಗಿಸುವ ರೀತಿ ಬಳಕೆದಾರರಿಗೆ ಸೇರಿದ್ದು.

ಸೈಬರ್ ಕೆಫೆಗೆ ಬರುವವರಲ್ಲಿ ಅಂತರ್ಜಾಲದಲ್ಲಿ ಕೆಲಸದ ಬೇಟೆ ಮಾಡಿ ತಮ್ಮ ಕಿರು ಪರಿಚಯಗಳನ್ನು ಫ್ಲಾಪ್ಪಿ ಯಿಂದ ವರ್ಗಾಯಿಸಿ ಅರ್ಜಿ ಹಾಕುವವರೂ ಇದ್ದಾರೆ. ಹಾಗೇ ಜೀವನದ ಜೋಡಿಯನ್ನು ಹುಡುಕಿ ಮದುವೆ ಅರ್ಜಿಯನ್ನು ಹಾಕುವವರೂ ಇದ್ದಾರೆ.

ದೂರ ದೇಶ ದಲ್ಲಿರುವ ತಮ್ಮ ಮೊಮ್ಮಕ್ಕಳು, ಮರಿ ಮಕ್ಕಳೊಡನೆ ವೀಡಿಯೋ ಹರಟೆ ಮಾಡುವವರೂ ಸೈಬರ್ ಕೆಫೆ ಗಳಲ್ಲಿ ಕಾಣ ಸಿಗುತ್ತಾರೆ.

ಪರೀಕ್ಷೆಯ ರಿಸಲ್ಟ್ ಬರುವ ಸಮಯದಲ್ಲಂತೂ ಅನೇಕರು ಸೈಬರ್ ಕೆಫೆಯಲ್ಲಿಯೇ ರಿಸಲ್ಟ್ ತಿಳಿದುಕೊಳ್ಳಲು ಬರುತ್ತಾರೆ.ತಿರುಪತಿ ದರ್ಶನಕ್ಕೆ ಸ್ಥಳ ಕಾದಿರಿಸುವವರೂ ರೈಲಿಗೆ ಸ್ಥಳ ಕಾದಿರಿಸುವವರೂ ಕೂಡ ಸೈಬರ್ ಕೆಫೆಗೆ ಬರುತ್ತಾರೆ.

ಸೈಬರ್ ಕೆಫೆಯ ಮೂಲಕ ದೇವರ ಪ್ರಾರ್ಥನೆಯನ್ನೂ ಮಾಡಬಹುದು, ಅಶ್ಲೀಲ ವೆಬ್ ಸೈಟ್ ಗಳನ್ನೂ ನೋಡಬಹುದು. ಆದ್ದರಿಂದ ಸೈಬರ್ ಕೆಫೆ ಗಳನ್ನು ನಾವು ಒಂದು ''ಅಂತರ್ಜಾಲ ಸೇವಾ ಕೇಂದ್ರ'' ವಾಗಿ ಪರಿಗಣಿಸಿ ಅವುಗಳು ಉಪಯುಕ್ತ ವಿಷಯಗಳನ್ನು ಜನರಿಗೆ ಹೆಚ್ಚು ಹೆಚ್ಚು ತರುವಂತೆ ಪ್ರೋತ್ಸಾಹಿಸಬೇಕಾದುದು ನಮ್ಮೆಲ್ಲರ ಕರ್ತವ್ಯ.

ಆದರೂ ಇಂದಿನ ನಿಜ ಸ್ಥಿತಿಯೇನೆಂದರೆ, ಇದುವರೆಗೆ ಸೈಬರ್ ಕೆಫೆ ಗಳ ಕೆಟ್ಟ ಮುಖ ಮಾತ್ರ ನಮ್ಮ ಗಮನಕ್ಕೆ ಬಂದಿದೆ. ಆದ್ದರಿಂದ ಸೈಬರ್ ಕೆಫೆಗಳನ್ನು ಕಠಿಣ ನಿಯಮಗಳ ಮೂಲಕ ನಿಯಂತ್ರಿಸಲು ಪ್ರಯತ್ನ ನಡೆಯುತ್ತಿದೆ.

ಸೈಬರ್ ಕೆಫೆಗಳು ತಮ್ಮ ವ್ಯವಹಾರದಲ್ಲಿ ಮುಂದುವರೆಯಬೇಕಾದರೆ, ಈ ನಿಯಮಗಳನ್ನು ಪರಿಚಯಿಸಿಕೊಂಡು ಅದನ್ನು ಮೀರದಂತೆ ನಡೆಯಬೇಕಾದುದು ಅಗತ್ಯ.

ಇಂತಹ ಸೈಬರ್ ಕೆಫೆ ನಿಯಂತ್ರಣ ನಿಯಮವನ್ನು ಇದೀಗ ಕರ್ನಾಟಕದಲ್ಲಿ ಕೂಡ ತರಲಾಗಿದೆ. ಈ ನಿಯಮಗಳ ಬಗ್ಗೆ ವಿವರಗಳನ್ನು ನಾವು ಈಗ ನೋಡೋಣ.

ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ (ಕರ್ನಾಟಕ) ನಿಯಮಗಳು–೨೦೦೪ ಎಂದು ಕರೆಯಲ್ಪಡುವ ಈ ನಿಯಮಗಳು (ನಾವು ಇದನ್ನು ಕರ್ನಾಟಕ ಸೈಬರ್ ಕೆಫೆ ನಿಯಮ ಎಂದು ಕರೆಯೋಣ), ಆಗಸ್ಟ್ ೫, ೨೦೦೪ ರಂದು ಹೊರತರಲಾದ ಕರ್ನಾಟಕ ಸರ್ಕಾರದ ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಮತ್ತು ಜೈವಿಕ ತಂತ್ರ ಜ್ಞಾನ ವಿಭಾಗದ ಸೂಚನೆಯಲ್ಲಿ ಅಡಕವಾಗಿದೆ. (ನಿಯಮ ಸೂಚನೆಯ ಪ್ರತಿಯನ್ನು ಪುಸ್ತಕದ ಕಡೆಯಲ್ಲಿ ಕೊಡಲಾಗಿದೆ.)

ಈ ಸೂಚನೆಗಳನ್ನು ಮಾತಂಕಾ ೨೦೦೦ ದ ಸೆಕ್ಷನ್ ೯೦ ರಲ್ಲಿ ರಾಜ್ಯ ಸರ್ಕಾರಕ್ಕೆ ಕೊಡಲ್ಪಟ್ಟಿರುವ ಅಧಿಕಾರದ ಮೇರೆಗೆ ಬಿಡುಗಡೆ ಮಾಡಲಾಗಿದೆ.

ಕರ್ನಾಟಕ ಸೈಬರ್ ಕೆಫೆ ನಿಯಮ ೨ (ಡಿ) ಪ್ರಕಾರ ಈ ನಿಯಮಗಳಲ್ಲಿ ''ಸೈಬರ್ ಕೆಫೆ'' ಎಂದರೆ ಸೈಬರ್ ಕೆಫೆ ಮಾಲಿಕ/ಜಾಲ ಸೇವಾ ದಾರ, ''ಅಂತರ್ಜಾಲ ಪ್ರವೇಶ ಸೇವೆ''ಯನ್ನೂ ಸೇರಿಸಿ ''ಕಂಪ್ಯೂಟರ್ ಸೇವೆ''ಗಳನ್ನು ಒದಗಿಸುವ ಸ್ಥಳ.

ಇದರಲ್ಲಿ ನಾವು ಗಮನಿಸಬೇಕಾದ ಅಂಶವೆಂದರೆ ಈ ನಿಯಮಗಳು ಸೈಬರ್ ಕೆಫೆಗಳಿಗಲ್ಲದೆ ಬೇರೆ ಕಂಪ್ಯೂಟರ್ ಸೇವೆಗಳಿಗೂ ಅನ್ವಯಿಸಲು

ಅವಕಾಶವಿರುತ್ತದೆ. ಅಂದರೆ ಕಾಲ್ ಸೆಂಟರ್, ಬಿ.ಪಿ.ಓ., ಐ.ಎಸ್.ಪಿ, ಅಂತರ್ಜಾಲ ಟೆಲಿಫೋನ್ ಸೇವೆ, ಸಾಮಾನ್ಯ ಟೆಲಿಫೋನ್ ಸೇವೆ ಗಳೂ ಈ ನಿಯಮದ ಚೌಕಟ್ಟಿನಲ್ಲಿ ಇರುವಂತೆ ಕಂಡು ಬರುತ್ತದೆ.

ಮಾತಂಕಾ ೨೦೦೦ ದಲ್ಲಿ ಜಾಲ ಸೇವಾದಾರ (ನೆಟ್ವರ್ಕ್ ಸರ್ವಿಸ್ ಪ್ರೊವೈಡರ್) ಎಂದರೆ ಯಾಹೂ, ಹಾಟ್ ಮೈಲ್, ರಿಡಿಫ್ಫ್ ಮೈಲ್, ಗೂಗಲ್ ಮೈಲ್ ಮುಂತಾದ ಸೇವಾದಾರರೆಂಬ ಅರ್ಥವನ್ನು ಕೊಡಲಾಗಿದೆ ಎಂಬುದನ್ನು ನಾವು ಇಲ್ಲಿ ನೆನಪಿಸಿಕೊಳ್ಳಬಹುದು.

ಬಹುಶಃ ಈ ಸೈಬರ್ ಕೆಫೆ ನಿಯಮಗಳನ್ನು ಈ ಎಲ್ಲಾ ರೀತಿಯ ಸೇವೆಗಳಿಗೂ ಅನ್ವಯಿಸಬೇಕೆಂಬುದು ಸರ್ಕಾರದ ಉದ್ದೇಶ ವಾಗಿರಲಾರದು ಎಂದು ನಮ್ಮ ಭಾವನೆ. ಇದರ ಬಗ್ಗೆ ಶ್ರೀಘ್ರದಲ್ಲೇ ಸರ್ಕಾರ ವಿವರಣೆಯನ್ನು ಕೊಡುತ್ತದೆಂದು ಆಶಿಸಿ ನಾವು ತಿಳಿದಿರುವ ಸೈಬರ್ ಕೆಫೆಗಳಿಗೆ ಈ ನಿಯಮಗಳು ಹೇಗೆ ಅನ್ವಯಿಸುತ್ತದೆ ಎಂಬ ಬಗ್ಗೆ ನಾವು ಈಗ ಗಮನ ಹರಿಸೋಣ.

ಈ ನಿಯಮಗಳಲ್ಲಿ ನಾವು ಗಮನಿಸಬೇಕಾದ ಮತ್ತೊಂದು ಮುಖ್ಯ ಅಂಶವೆಂದರೆ ನಿಯಮ ೨ (ಇ) ಪ್ರಕಾರ ಸೈಬರ್ ಪೋಲೀಸ್ ಅಥಾರಿಟಿ ಎಂದರೆ ಸೈಬರ್ ಕ್ರೈಂ ಪೋಲೀಸ್ ಸ್ಟೇಷನ್ ಎಂಬುದು. ಸೈಬರ್ ಪೋಲೀಸ್ ಸ್ಟೇಷನ್ ಈಗ ಬೆಂಗಳೂರಿನಲ್ಲಿದ್ದು ಅದಕ್ಕೆ ರಾಜ್ಯ ಪೂರಾ ಅಧಿಕಾರ ವ್ಯಾಪ್ತಿಯನ್ನು ಕೊಡಲಾಗಿದೆ.

ಆದ್ದರಿಂದ ಈ ನಿಯಮಗಳ ಪ್ರಕಾರ ಸೈಬರ್ ಕೆಫೆಗಳನ್ನು ತಪಾಯಿಸುವ ಹಕ್ಕು ಸೈಬರ್ ಕ್ರೈಂ ಪೋಲೀಸ್ ಸ್ಟೇಷನ್ ಗೆ ಮಾತ್ರ ಇರುತ್ತದೆ ಎಂದು ನಾವು ಅರ್ಥೈಸಬಹುದು.

ಕರ್ನಾಟಕದಲ್ಲಿ ಇದೆ ಎನ್ನಲಾದ ೫೦,೦೦೦ ಸೈಬರ್ ಕೆಫ಼ೆಗಳನ್ನು ಬೆಂಗಳೂರಿನಲ್ಲಿರುವ ಒಂದು ಪೋಲೀಸ್ ಸ್ಟೇಷನ್ ನಿಂದ ನಿಯಂತ್ರಿಸುವುದು ಸಾಧ್ಯವೇ ಎಂಬುದು ಸರ್ಕಾರ ಗಮನಿಸಬೇಕಾದ ವಿಷಯ.

ನಿಯಮ ೩ (೧) ರ ಪ್ರಕಾರ ಸೈಬರ್ ಕೆಫ಼ೆ ಮಾಲಿಕ ತನ್ನಲ್ಲಿರುವ ಕಂಪ್ಯೂಟರ್ ಮತ್ತು ವ್ಯವಸ್ಥೆ ಯನ್ನು ಯಾವುದೇ ಕಾನೂನು ಬಾಹಿರ ಅಥವಾ ಅಪರಾಧ ಕೃತ್ಯಗಳಿಗೆ ಬಳಸದಂತೆ ಸಂಪೂರ್ಣ ಎಚ್ಚರಿಕೆಯನ್ನು ವಹಿಸಬೇಕು.

''ಸಂಪೂರ್ಣ ಎಚ್ಚರಿಕೆ''ಯ ವ್ಯಾಪ್ತಿ ಎಷ್ಟು ಎಂಬುದು ನಿಯಮದಲ್ಲಿ ಸ್ಪಷ್ಟ ಪಡಿಸಿಲ್ಲ. ಆದರೂ ಸೈಬರ್ ಕೆಫ಼ೆ ಮಾಲಿಕರು ''ಕಾನೂನು ಬಾಹಿರ'' ಅಥವಾ ''ಅಪರಾಧ'' ಎಂದರೆ ಏನು ಎಂಬುದನ್ನು ತಿಳಿಯಬೇಕಾದುದು ಅತ್ಯಗತ್ಯ. ಈ ದಿಸೆಯಲ್ಲಿ ಈ ಪುಸ್ತಕ ಸಹಾಯವಾಗಬಹುದೆಂದು ನಮ್ಮ ಅನಿಸಿಕೆ.

ನಿಯಮ-೩(೧) ರಲ್ಲಿ, ನಿಯಮ-೨ ರಲ್ಲಿ ಉಪಯೋಗಿಸಿರುವಂತೆ ''ಸೈಬರ್ ಕೆಫ಼ೆ ಮಾಲಿಕ/ಜಾಲ ಸೇವಾದಾರ'' ಎಂಬ ಪದವನ್ನು ಉಪಯೋಗಿಸದೆ ಬರೀ ''ಸೈಬರ್ ಕೆಫ಼ೆ ಮಾಲಿಕ'' ಎಂಬ ಪದ ಪ್ರಯೋಗ ಮಾಡಿರುವುದು ಈ ''ಸಂಪೂರ್ಣ ಎಚ್ಚರಿಕೆ'' ನಿಯಮ ಐ.ಎಸ್.ಪಿ, ಬಿ.ಪಿ.ಓ., ಮುಂತಾದ ಜಾಲ ಸೇವಾದಾರರಿಗೆ ಅನ್ವಯವಾಗುವುದಿಲ್ಲವೋ ಎಂಬ ಭಾವನೆಯನ್ನು ನೀಡುತ್ತದೆ.

ನಿಯಮ ೩ (೨) ರ ಪ್ರಕಾರ ಸೈಬರ್ ಕೆಫ಼ೆ ಮಾಲಿಕ ಅಥವಾ ಜಾಲ ಸೇವಾದಾರ, ಬಳಕೆದಾರ ತನ್ನ ಗುರುತನ್ನು ಆ ಮಾಲಿಕ/ಸೇವಾದಾರನ ಎದುರಿಗೆ ಪ್ರತಿಪಾದಿಸುವುದಕ್ಕೆ ಮುನ್ನ, ತನ್ನ ಕಂಪ್ಯೂಟರ್, ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ಜಾಲವನ್ನು ಬಳಸುವುದಕ್ಕೆ ಅವಕಾಶ ಕೊಡಬಾರದು.

ಸೇವಾಕಾಂಕ್ಷಿ ತನ್ನ ಗುರುತನ್ನು ಸೈಬರ್ ಕೆಫೆ ಮಾಲಿಕ/ಜಾಲ ಸೇವಾದಾರನಿಗೆ ಒಪ್ಪಿಗೆಯಾಗುವಂತೆ, ಶಾಲೆ, ಕಾಲೇಜಿನಲ್ಲಿ ನೀಡಿದ ಫೋಟೋಯುಕ್ತ ಗುರುತಿನ ಚೀಟಿಯನ್ನಾಗಲೀ, ಫೋಟೋ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡನ್ನಾಗಲೀ, ಬ್ಯಾಂಕ್, ಪಾಸ್ ಪೋರ್ಟ್, ಅಥವಾ ಮತದಾರ ಗುರುತಿನ ಚೀಟಿ ಅಥವಾ ವರಮಾನ ಇಲಾಖೆ ಕೊಟ್ಟ ಪ್ಯಾನ್ ಕಾರ್ಡ್ ಆಗಲೀ, ಅಥವಾ ಕೆಲಸಗಾರನ ಗುರುತಿನ ಕಾರ್ಡ್ ಆಗಲೀ, ಅಥವಾ ವಾಹನ ಚಾಲನೆ ಲೈಸೆನ್ಸ್ ಆಗಲೀ ಉಪಯೋಗಿಸಿ ಪ್ರತಿಪಾದಿಸಬಹುದು.

ಈ ನಿಯಮದಲ್ಲಿ ಜಾಲ ಸೇವಾದಾರ ತನ್ನ ಸೇವೆಯನ್ನು ಕಂಪ್ಯೂಟರ್ ಜಾಲದ ಮೂಲಕ ನೀಡುತ್ತಿದ್ದರೆ, ಬಳಕೆದಾರರನ್ನು ಪಾಸ್ ವರ್ಡ್ ಮುಖಾಂತರ ಗುರಿತಿಸಬಹುದೇ ಅಥವಾ ಡಿಜಿಟಲ್ ಸಹಿಯ ಮುಖಾಂತರ ಗುರುತಿಸಬಹುದೇ ಎಂಬ ಬಗ್ಗೆ ವಿವರಣೆ ಇಲ್ಲ.

ನಿಯಮ ೪ (೧) ರ ಪ್ರಕಾರ ಬಳಕೆದಾರನ ಗುರುತನ್ನು ಪ್ರತಿಪಾದಿಸಿದ ಮೇಲೆ, ಸೈಬರ್ ಕೆಫೆ ಮಾಲಿಕ ಅಥವಾ ನಿರ್ವಾಹಕ ಅಥವಾ ಪರಿಚಾರಕ ಅಥವಾ ಅವನ ಪರವಾಗಿ ಅಧಿಕರಿಸಲ್ಪಟ್ಟ ಸೈಬರ್ ಕೆಫೆ ನಿರ್ವಹಿಸುವ ವ್ಯಕ್ತಿ ಈ ಕೆಳಕಂಡ ಮಾಹಿತಿಯನ್ನು ಪಡೆದು ಅದನು ್ನ"ಲಾಗ್ ರಿಜಿಸ್ಟರ್" ನಲ್ಲಿ ಬರೆದಿಡಬೇಕು.

೧. ಬಳಕೆದಾರನ ಹೆಸರು
೨. ಬಳಕೆದಾರನ ವಯಸ್ಸು ಮತ್ತು ಲಿಂಗ
೩. ಬಳಕೆದಾರನ ಈಗಿನ ವಾಸಸ್ಥಳದ ವಿಳಾಸ
೪. ಒಳಗೆ ಬಂದ ಸಮಯ
೫. ಹೊರಗೆ ಹೋದ ಸಮಯ

ಈ ನಿಯಮದಲ್ಲಿ ನಾವು ಗಮನಿಸಬೇಕಾದ ಅಂಶವೆಂದರೆ, ಈ ರಿಜಿಸ್ಟರನ್ನು ಯಾವುದೇ ಪರಿಚಾರಕ ಬರೆಯಬಹುದು ಹಾಗೂ ನಿಯಮ ೩(೨) ರಲ್ಲಿ ಗುರುತನ್ನು ಮಾಲೀಕನ ಎದುರು ಮಾತ್ರ ಪ್ರತಿಪಾದಿಸಬಹುದೆಂದು ತಿಳಿಸಲಾಗಿದ್ದರೂ, ಲಾಗ್ ರಿಜಿಸ್ಟರನ್ನು ಯಾರು ಬೇಕಾದರೂ ಬರೆಯಬಹುದೆಂದು ತಿಳಿಸಿರುವುದು.

ಈ ನಿಯಮದಲ್ಲಿ ಬಳಕೆದಾರನ ಸಹಿ ಮತ್ತು ಗುರುತನ್ನು ಪ್ರತಿಪಾದಿಸಿದ ವಿಧಾನದ ಬಗ್ಗೆ ಬರೆಯಬೇಕೆಂದು ತಿಳಿಸಿಲ್ಲ. ಆದರೂ ನಿಯಮದ ಕಡೆಯಲ್ಲಿ ಕೊಡಲಾದ ಫ್ಲಾರಂ–೧ ರ ರೂಪವನ್ನು ನೋಡಿದರೆ ಗುರುತು ಪ್ರತಿಪಾದಿಸಿದ ವಿಧಾನ, ಮತ್ತು ಬಳಕೆದಾರನ ಸಹಿ ಅಗತ್ಯವೆನ್ನಬಹುದು.

ನಿಯಮದ ಕಡೆಯಲ್ಲಿ ಕೊಟ್ಟಿರುವ ಫ್ಲಾರಂ–೧ ರ ರೂಪ ಕೆಳಕಂಡಂತೆ ಇದೆ.

FORM No. 1

Sl. No.	Machine No.	Name, Age, Sex and address of the User	Signature	Log in time	Log out time	Type of ID produced	Issued by whom	Remarks
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)

ಮೇಲೆ ಕೊಟ್ಟಿರುವ ಫ್ಲಾರಂ ನಲ್ಲಿ ಬಳಕೆದಾರ ತನ್ನ ಹೆಸರು, ವಯಸ್ಸು, ಲಿಂಗ, ಮತ್ತು ವಿಳಾಸ (ಕಲ್ಂ ೩) ವನ್ನು ತನ್ನ ಹಸ್ತಾಕ್ಷರದಲ್ಲೇ ಬರೆದು ಕಲ್ಂ ೪ ರಲ್ಲಿ ಸಹಿ ಮಾಡಬೇಕೆಂದು ನಿಗದಿಸಿದೆ.

ನಿಯಮ ೪(೨) ರ ಪ್ರಕಾರ ಬಳಕೆದಾರ ನಿಯಮ ೩ (೨) ರಲ್ಲಿ ತಿಳಿಸಿರುವಂತೆ ಸೈಬರ್ ಕೆಫೆ ಮಾಲಿಕ ಅಥವಾ ಜಾಲಸೇವಾ ದಾರನ ಅವಶ್ಯಕತೆಯಂತೆ ಗುರುತನ್ನು ಪ್ರತಿಪಾದಿಸಲಾಗದಿದ್ದರೆ, ಬಳಕೆದಾರನ ಅನುಮತಿಯಿಂದ ಸೈಬರ್ ಕೆಫೆ ಯ ಕಂಪ್ಯೂಟರ್ ಗೆ ಅಳವಡಿಸಿದ ''ವೆಬ್ ಕ್ಯಾಮೆರ'' ಉಪಯೋಗಿಸಿ ಅವನ ಫೋಟೊ ತೆಗೆದುಕೊಳ್ಳಬಹುದು.

ಈ ಅನುಮತಿಯನ್ನು ಪಡೆಯುವಾಗ, ಫೋಟೊವನ್ನು ಕಂಪ್ಯೂಟರ್ ನ ಹಾರ್ಡ್ ಡಿಸ್ಕ್ ನಲ್ಲಿ ಶೇಖರಿಸಿಟ್ಟು ಬೇಕಾದಾಗ ಕಾನೂನು ಜಾರಿ ಮಾಡುವ ಅಧಿಕಾರಿಗಳಿಗೆ ಒದಗಿಸಬಹುದೆಂದು ತಿಳಿಸಬೇಕು. (ಇಲ್ಲಿ ಕಾನೂನು ಜಾರಿ ಮಾಡುವ ಅಧಿಕಾರಿ ಎಂದರೆ ಪೋಲೀಸ್ ಎಂದು ಅರ್ಥೈಸಬಹುದು.)

ಇದಕ್ಕೆ ಬಳಕೆದಾರ ಒಪ್ಪದಿದ್ದರೆ ಅವನು ಸೈಬರ್ ಕೆಫೆಯ ಯಾವುದೇ ಕಂಪ್ಯೂಟರ್, ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆ ಅಥವಾ ಜಾಲವನ್ನು ಉಪಯೋಗಿಸುವುದಕ್ಕೂ ಅಂತರ್ಜಾಲಕ್ಕೆ ಪ್ರವೇಶ ಪಡೆಯುವುದಕ್ಕೂ ಅವಕಾಶ ಕೊಡುವಂತಿಲ್ಲ.

ನಿಯಮ ೪(೩) ರ ಪ್ರಕಾರ ಸೈಬರ್ ಕೆಫೆಯಲ್ಲಿರುವ ಎಲ್ಲಾ ಗಡಿಯಾರಗಳನ್ನೂ ಆಗಾಗ್ಗೆ ಪರಿಶೀಲಿಸಿ ಭಾರತೀಯ ಕಾಲಮಾನಕ್ಕೆ ಹೊಂದಿಸಿಡಬೇಕು. (ಈ ನಿಯಮದಲ್ಲಿ ಹೇಳಿರುವ ಗಡಿಯಾರ ಎಂದರೆ ಕಂಪ್ಯೂಟರ್ ಒಳಗಿನ ಗಡಿಯಾರ ಎಂದು ಅರ್ಥೈಸಬೇಕು).

ನಿಯಮ ೪(೪) ರ ಪ್ರಕಾರ ಬಳಕೆದಾರರ ಬಗ್ಗೆ ಸರಿಯಾದ ವಿವರಗಳನ್ನು ಇಡುವುದು ಸೈಬರ್ ಕೆಫೆ ಮಾಲಿಕ ಅಥವಾ ಸೇವಾದಾರನ ಜವಾಬ್ದಾರಿ.

ನಿಯಮ ೪(೫) ರ ಪ್ರಕಾರ ಲಾಗ್ ರಿಜಿಸ್ಟರ್ ಮತ್ತು ಬಳಕೆದಾರನ ಫೋಟೊ ವನ್ನು ಕನಿಷ್ಟ ಒಂದು ವರ್ಷ ಕಾಲ ಉಳಿಸಿಟ್ಟಿರಬೇಕು ಮತ್ತು ಅಗತ್ಯ ಬಿದ್ದಾಗ ಕಾನೂನು ಜಾರಿಮಾಡುವ ಅಧಿಕಾರಿಗಳಿಗೆ ಒದಗಿಸಬೇಕು.

ನಿಯಮ ೪(೬)ರ ಪ್ರಕಾರ ಸೈಬರ್ ಪೋಲೀಸ್ ಅಧಿಕಾರಿಗಳು ದೂರಿನ ಮೇಲೆ ಸೈಬರ್ ಕೆಫೆಯನ್ನು ಪರೀಕ್ಷೆ ಮಾಡಬಹುದು. ಯಾವುದೇ ಸೈಬರ್ ಕೆಫೆ ಮಾಲಿಕ ಅಥವಾ ಜಾಲ ಸೇವಾದಾರ ಲಾಗ್ ರಿಜಿಸ್ಟರ್ ಮತ್ತು ದಾಖಲೆಗಳನ್ನು ಇಟ್ಟಿಲ್ಲದಿದ್ದರೆ ಅವನು ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯಿದೆ ೨೦೦೦ ದ ಪ್ರಕಾರ ಅಥವಾ ಬೇರಾವುದಾದರೂ ಕಾನೂನಿನ ಮೇರೆಗೆ ದಂಡನೆಗೆ ಅರ್ಹನಾಗುತ್ತಾನೆ.

ಈ ನಿಯಮದ ಚೌಕಟ್ಟಿನಲ್ಲಿ ಬರುವುದು ಮಾತಂಕಾ–೨೦೦೦ ದ ಸೆಕ್ಷನ್ ೬೫. ಇದರಲ್ಲಿರುವ ದಂಡನೆ ೩ ವರ್ಷ ಸೆರೆವಾಸ ಮತ್ತು ರೂಪಾಯಿ ೧ ಲಕ್ಷ ದಂಡದ ಸಾಧ್ಯತೆ ಎಂಬುದನ್ನು ಗಮನಿಸಬೇಕು.

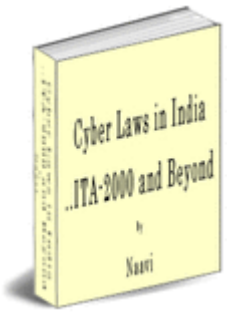
ಈಗಾಗಲೇ ತಿಳಿಸಿರುವಂತೆ ಈ ನಿಯಮಗಳ ಪ್ರಕಾರ ಬೆಂಗಳೂರು ಸೈಬರ್ ಕ್ರೈಂ ಪೋಲೀಸ್ ಸ್ಟೇಷನ್ ಅಧಿಕಾರಿಗಳಿಗೆ ಮಾತ್ರ ಸೈಬರ್ ಕೆಫೆ ಗಳ ಪರೀಕ್ಷಣೆಗೆ ಅವಕಾಶವಿರುತ್ತದೆ. ಇತರ ಸ್ಥಳೀಯ ಪೋಲೀಸ್ ಅಧಿಕಾರಿಗಳಿಗೆ ಈ ಅಧಿಕಾರವಿರುವುದಿಲ್ಲ.

ಕರ್ನಾಟಕದಲ್ಲಿ ಸೈಬರ್ ಕೆಫೆ ನಿಯಂತ್ರಣ ತರುವುದಕ್ಕೆ ಬಹಳ ಮುಂಚೆಯೇ ಮಹಾರಾಷ್ಟ್ರ ದಲ್ಲಿ ಸೈಬರ್ ಕೆಫೆ ನಿಯಂತ್ರಣವನ್ನು ತರಲಾಯಿತು. ಇದು ಮುಖ್ಯವಾಗಿ ಸೈಬರ್ ಕೆಫೆ ನೊಂದಾವಣೆ, ಸೈಬರ್ ಕೆಫೆ ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆಯಲ್ಲಿನ ಆಸ್ಥಿ ವಿವರಗಳ ನೊಂದಾವಣೆ, ದೈನಂದಿಕ ವ್ಯವಹಾರಗಳ ವರದಿ ಮುಂತಾದ ವಿಷಯಗಳನ್ನು ಒಳಗೊಂಡಿತ್ತು. ಆದರೆ ಈ ನಿಯಂತ್ರಣ ವ್ಯವಸ್ಥೆ ಅಷ್ಟೇನೂ ಯಶಸ್ವಿಯಾದಂತೆ ಕಾಣಬಂದಿಲ್ಲ. ಇಂದಿಗೂ ಅಲ್ಲಿಯ ಸೈಬರ್ ಕೆಫೆಗಳು

ಸರಿಯಾದ ಮಾಹಿತಿಯನ್ನು ಅಪರಾಧ ಸಮಯದಲ್ಲಿ ಪೋಲೀಸರಿಗೆ ಒದಗಿಸುವುದರಲ್ಲಿ ವಿಫಲವಾಗಿವೆ.

ಅಹಮದಾಬಾದ್, ಮೀರತ್ ಮತ್ತು ಕೆಲವೆಡೆಗಳಲ್ಲಿ ಸೈಬರ್ ಕೆಫೆಗಳಲ್ಲಿ ಕ್ಯಾಬಿನ್ ಗಳನ್ನು ವಿರೋಧಿಸಿ ಪೋಲೀಸರು ಕ್ರಮ ಜರುಗಿಸಿದ್ದುಂಟು. ಇನ್ನು ಕೆಲವೆಡೆ ಗ್ರಾಹಕರು ಅಶ್ಲೀಲ ಚಿತ್ರಗಳನ್ನು ನೋಡಿದ ಅಪರಾಧದ ಮೇಲೆ ಸೈಬರ್ ಕೆಫೆ ಮಾಲಿಕರನ್ನು ಬಂಧಿಸಿ ಕ್ರಮ ಜರುಗಿಸಿದ ಪ್ರಸಂಗಗಳೂ ಇವೆ. ಈ ಪ್ರಸಂಗಗಳಾವುದೂ ನ್ಯಾಯಾಲಯದಲ್ಲಿ ಅಪರಾಧವೆಂದು ಪರಿಗಣಿಸಲ್ಪಟ್ಟು ತೀರ್ಪು ಹೊರಬಂದ ವಾರ್ತೆ ಲಭ್ಯವಾಗಿಲ್ಲ.

ಈ ಹಿನ್ನಲೆಯಲ್ಲಿ ಕರ್ನಾಟಕದ ಸೈಬರ್ ಕೆಫೆ ನಿಯಂತ್ರಣ ಎಷ್ಟು ಯಶಸ್ವಿಯಾಗುತ್ತದೆಯೆಂಬುದನ್ನು ಕಾದು ನೋಡಬೇಕು. ಈ ರೀತಿಯ ಕಾನೂನು ಯಶಸ್ವಿಯಾಗಬೇಕಿದ್ದರೆ ಜನರಿಗೆ ಇದರ ಬಗ್ಗೆ ತಿಳುವಳಿಕೆ ಕೊಡಬೇಕಾದದ್ದು ಬಹಳ ಮುಖ್ಯ. ಈ ತಿಳುವಳಿಕೆ ಕೊಡುವ ಜವಾಬ್ದಾರಿ ಸರ್ಕಾರದ್ದು ಎಂದರೆ ತಪ್ಪಲ್ಲ.



http://www.naavi.org

Annexure

GOVERNMENT OF KARNATAKA

No: ITD 07 PRM 2004

Karnataka Government Secretariat,
Department of Information Technology & Biotechnology
UNI Building, Thimmaiah Road,
Bangalore,

dated: 05.08.2004.

NOTIFICATION

In exercise of the powers conferred by section 90 of the Information Technology Act, 2000 (Central Act 21 of 2000), the Government of Karnataka hereby makes the following rules, namely:

1.Title and Commencement:

(1). These rules may be called the Information Technology (Karnataka) Rules 2004.

(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 (Central Act 21 of 2000);

(b) "Log Register" means the Register in Form-1 maintained by the Cyber Café owner/Network Service Provider for using the Cyber Café.

(c) "User" means a person who uses the Computer in a Cyber Café

(d) "Cyber Café" means a premises where the Cyber Café Owner/Network Service Provider provides the computer services including Internet access to the public.

(e) Cyber Police Authority" means the officers of the Cyber Crime Police Station.

3. Cyber Café:

(1) The owner of the Cyber Café shall take sufficient precautions so that computers and computer systems in the Cyber Café are not used for any illegal or criminal activity.

(2) Cyber Café Owner/Network Service Provider shall not allow any User to use his Computer, Computer System and/or Computer Network without the identity of the User being established before him before use. The intending User may establish his Identity by producing any Photo Identity Card issued by any School or College or a Photo Credit Card of any Bank or Passport or Voters Identity Card or PAN Number Card issued by Income-Tax authorities or Photo Identity Card issued by the Employer or Driving License to the satisfaction of Cyber Café Owner.

4. Entries in the Log Register:

(1) After the Identity of the User is established, the owner of the Cyber Café or the manager or the attendant or on his behalf any authorised person managing the Cyber Café shall obtain and maintain the following information in the Log Register for each user:

i. Name of the User
ii. Age and Sex of the User
iii. Present residential address of the User
iv. Log in time
v. Log out time

(2) When a User cannot produce any Photo Identity Card to establish his identity to the satisfaction of the Cyber Café Owner/Network Service Provider, he may be photographed by the Cyber Café Owner/Network Service Provider after obtaining his consent using a

'Web Camera' hooked onto one of the computers or computer systems in the Cyber Café and the User shall be explained that his photograph will be taken and stored in the hard disk of the computer, for verification by Law enforcement authorities, whenever required. This is in addition to the entries made in the log register. In case the User does not agree for storing his photograph he shall not be allowed to use any computer, computer system and /or computer network or access to the Internet in the Cyber Café.

(3) All time clocks in Cyber Cafes must be regularly checked and synchronized with Indian Standard Time (IST).

(4) Maintaining proper account of the User as explained shall be the responsibility of the Cyber Café Owner/Network Service provider.

5) Log Register and the Photograph of the User shall be maintained by the Cyber Café Owner/Network Service Provider for a minimum period of ONE YEAR and which shall be provided to Law enforcement agencies as and when required.

(6) Cyber Police authorities may on complaint inspect Cyber Cafes at all reasonable time to ensure compliance of these rules. If any Cyber Café Owner/Network Service Provider fails to maintain Log Register and records he shall be liable for penalties as provided in the Act or any other Law, for the time being in force.

By Order and in the Name of the Governor of Karnataka,

(K M Ananda)
Under Secretary to Government Dept. of IT, BT and Science & Technology

FORM No. 1

Sl. No.	Machine No.	Name, Age, Sex and address of the User	Signature	Log in time	Log out time	Type of ID produced	Issued by whom	Remarks
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)

Note: Column No.3 and 4 will be written by the User in his/her own handwriting and the remaining columns are to be entered by the owner of the cyber Café or manager or attendant of Cyber Café.

Disclaimer

This book contains translations of some of the provisions of Acts published in English. It is hereby notified that the translations are for the purpose of clarification only and not to be treated as official versions of the Act. Sufficient care has been taken to publish the book free from errors. Comments are made to the best of the author's understanding and belief. However the contents of this book are not to be treated as legal advise and the Authors or the Publishers will not be liable for any action taken by readers based on the contents of this book

http://www.naavi.org

ಲೇಖಕರ ಪರಿಚಯ

ನಾವಿ ಎಂಬುದು ನಾ.ವಿಜಯಶಂಕರ ರವರ ಅಂತರ್ಜಾಲ ನಾಮ. ಮೈಸೂರಿನಲ್ಲಿ ಜನಿಸಿ ೧೯೭೩ ನೇ ಇಸವಿಯಲ್ಲಿ ಮಾನಸ ಗಂಗೋತ್ರಿಯಲ್ಲಿ ಫಿಸಿಕ್ಸ್ ವಿಭಾಗದಲ್ಲಿ ಎಂ.ಎಸ್.ಸಿ. ಪದವಿಯನ್ನು ಪಡೆದ ನಾವಿ ಈಗ ಚೆನ್ನೈ ನಲ್ಲಿ ವಾಸವಾಗಿದ್ದಾರೆ. ೩೦ ವರ್ಷಕ್ಕೂ ಹೆಚ್ಚು ಕಾಲ ಬ್ಯಾಂಕ್ ಮತ್ತು ಇತರ ನಿರ್ವಹಣೆಗಳಲ್ಲಿ ಅಧಿಕಾರಿಗಳಾಗಿ ಕೆಲಸ ಮಾಡಿರುವ ನಾವಿ ಇಂದು ಭಾರತದ ಸೈಬರ್ ಕಾನೂನಿನ ತಜ್ಞ ರಲ್ಲೊಬ್ಬರೆಂದು ಪರಿಗಣಿಸಲ್ಪಟ್ಟಿದ್ದಾರೆ.

೧೯೯೯ ರಲ್ಲಿ ಸೈಬರ್ ಕಾನೂನಿನ ಬಗ್ಗೆ ಭಾರತದ ಮೊದಲ ಪುಸ್ತಕವನ್ನು ಪ್ರಕಟಿಸಿದ ಖ್ಯಾತಿ ಪಡೆದ ನಾವಿ, ೨೦೦೩ ರಲ್ಲಿ ಇದೇ ವಿಷಯದ ಭಾರತದ ಮೊದಲ ಇ-ಪುಸ್ತಕವನ್ನು ಕೂಡ ಹೊರತಂದರು. ಇತ್ತೀಚೆಗೆ ಇವರ ಮೂರನೇ ಪುಸ್ತಕ ಕೂಡ ಹೊರಬಂದಿದೆ.

www.naavi.org ಮತ್ತು www.cyberlawcollege.com ಎಂಬ ವೆಬ್ ಸೈಟ್ ಗಳ ಮೂಲಕ ಸೈಬರ್ ಕಾನೂನಿನ ಜ್ಞಾನವನ್ನು ಜನ ಸಾಮಾನ್ಯರಿಗೆ ತಲುಪಿಸುತ್ತಿರುವ ನಾವಿ, ಚೆನ್ನೈ ಪೋಲೀಸರಿಗೆ ಸೈಬರ್ ಅಪರಾಧಗಳ ಬಗ್ಗೆ ಶಿಕ್ಷಣ ಕೊಟ್ಟು ಅಪರಾಧಗಳ ತನಿಖೆಗಳಲ್ಲಿ ಸಹಾಯ ಒದಗಿಸುತ್ತಿದ್ದಾರೆ.

ಕೇಂದ್ರ ಸರ್ಕಾರದ ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಇಲಾಖೆಯ ಸೈಬರ್ ಕಾನೂನಿಗೆ ಸಂಬಂಧ ಪಟ್ಟ ಕೆಲವು ಸಮಿತಿಗಳಲ್ಲಿ ಸದಸ್ಯರಾಗಿ ಸೇವೆ ಸಲ್ಲಿಸಿರುವ ನಾವಿ ರವರು ಪ್ರಸ್ತುತ ಕರ್ನಾಟಕ ಸರ್ಕಾರದ ಇ-ಆಡಳಿತ ಸಮಿತಿಯಲ್ಲೂ ಸದಸ್ಯರಾಗಿ ತಮ್ಮ ಅನುಭವವನ್ನು ಹಂಚಿಕೊಳ್ಳುತ್ತಿದ್ದಾರೆ.

http://www.naavi.org

"ಕಾನೂನು ಮಾಡುವುದು ಸರ್ಕಾರದ ಕೆಲಸ. ಅದನ್ನು ತಿಳಿದುಕೊಳ್ಳುವುದು ಪ್ರಜೆಯ ಜವಾಬ್ದಾರಿ"

ಮಾತಂಕಾ–೨೦೦೦ ಭಾರತದಲ್ಲಿ ಕಾನೂನಿನ ರೂಪಕ್ಕೆ ಬಂದು ೪ ವರ್ಷಗಳು ಕಳೆದಿವೆ. ಇತ್ತೀಚೆಗೆ ಕರ್ನಾಟಕದಲ್ಲಿ ಸೈಬರ್ ಕೆಫೆಗಳ ನಿಂಯಂತ್ರಣಕ್ಕೆ ಹೊಸ ನಿಯಮಗಳನ್ನು ಸರ್ಕಾರ ಹೊರಡಿಸಿದೆ. ಈ ಸಂದರ್ಭದಲ್ಲಿ ಅಂತರ್ಜಾಲ ಅಪರಾಧಗಳೆಂದರೇನು? ಅವುಗಳು ಜನ ಸಾಮಾನ್ಯರ ಮೇಲೆ ಮತ್ತು ಸೈಬರ್ ಕೆಫೆಗಳ ಮೇಲೆ ಬೀರುವ ಪರಿಣಾಮವೇನು? ಎಂಬುದನ್ನು ತಿಳಿದುಕೊಳ್ಳುವುದು ಅವಶ್ಯಕ.

ಅಲ್ಲದೆ ಇಂದು ಹಲವಾರು ಸೈಬರ್ ಅಪರಾಧಗಳಲ್ಲಿ ಅಪ್ರಾಪ್ತ ವಯಸ್ಕರು ಮತ್ತು ಕಾಲೇಜ್ ಯುವಕ ಯುವತಿಯರು ಸಿಕ್ಕಿ ಬೀಳುತ್ತಿರುವುದು ಆತಂಕದ ವಿಷಯ. ಇದನ್ನು ಕಡಿಮೆ ಮಾಡಬೇಕಾದರೆ ಕಂಪ್ಯೂಟರ್ ಬಗ್ಗೆ ಪಾಠ ಮಾಡುವ ಶಾಲೆಗಳಲ್ಲೆಲ್ಲಾ ಸೈಬರ್ಾಪರಾಧಗಳ ಬಗ್ಗೆ ಕೂಡ ಪಾಠ ಮಾಡುವುದು ಅವಶ್ಯ.

ಇಂದು ಕರ್ನಾಟಕ ಸರ್ಕಾರ ಅನೇಕ ಇ–ಆಡಳಿತ ಸೇವೆಗಳನ್ನು ಜನಗಳಿಗೆ ಕೊಡುತ್ತಾ ಬಂದಿದೆ. ಇದರಲ್ಲಿ "ಭೂಮಿ" ಯಂತಹ ಸೇವೆಗಳು ಹಳ್ಳಿ ಹಳ್ಳಿಗಳಲ್ಲೂ ಕಂಪ್ಯೂಟರ್ ಬಳಕೆ ಹೆಚ್ಚುವಂತೆ ಮಾಡಿದೆ. ಇದರಿಂದ ಇಂಗ್ಲಿಷ್ ಬರದ ಕನ್ನಡಿಗರಿಗೆ ಕೂಡ ಅಂತರ್ಜಾಲದ ಕಾನೂನಿನ ಬಗ್ಗೆ ಸಾಮಾನ್ಯ ಜ್ಞಾನ ಇರಬೇಕಾದುದು ಅತ್ಯವಶ್ಯಕ.

ಈ ಎಲ್ಲಾ ವಿಚಾರಗಳನ್ನು ಗಮನದಲ್ಲಿಟ್ಟುಕೊಂಡು ಸೈಬರ್ ಅಪರಾಧಗಳ ವಿಚಾರವನ್ನು ಆದಷ್ಟು ಜನ ಸಾಮಾನ್ಯರಿಗೆ ಅರ್ಥವಾಗುವಂತೆ ಈ ಪುಸ್ತಕದಲ್ಲಿ ಬರೆಯಲಾಗಿದೆ.

ಭಾರತದಲ್ಲಿಯೇ ಪ್ರಥಮ ಬಾರಿಗೆ ರಾಜ್ಯ ಭಾಷೆಯೊಂದರಲ್ಲಿ ಸೈಬರ್ ಕಾನೂನಿನ ಬಗ್ಗೆ ಪುಸ್ತಕ ಕನ್ನಡ ದಲ್ಲಿ ದೊರಕಿರುವುದು, ರಾಷ್ಟ್ರದಲ್ಲೇ ಮೊದಲ ಸೈಬರ್ ಕ್ರೈಂ ಪೋಲೀಸ್ ಸ್ಟೇಶನ್ ತೆರೆದ ಖ್ಯಾತಿಯನ್ನು ಪಡೆದ ಕರ್ನಾಟಕಕ್ಕೆ ತಕ್ಕ ಬೆಳವಣಿಗೆಯೆನ್ನಬಹುದು.