ಭಾರತದ ಸೈಬರ್ ಕಾನೂನು ಚೌಕಟ್ಟು: ಉದಯೋನ್ಮುಖ ಸೈಬರ್ ಅಪರಾಧಗಳು ಮತ್ತು ತಾಂತ್ರಿಕ ಸವಾಲುಗಳ ಕಾನೂನುಬದ್ಧ ವಿಶ್ಲೇಷಣೆ

ನಾಗೇಂದ್ರಪ್ಪ ಕೆ.ಟಿ.

ಸಹ ಪ್ರಾಧ್ಯಾಪಕರು, ರಾಜ್ಯಶಾಸ್ತ್ರ ವಿಭಾಗ, ವೈ.ಡಿ.ಡಿ. ಸರ್ಕಾರಿ ಪ್ರಥಮ ದರ್ಜೆ ಕಾಲೇಜು, ಬೇಲೂರು.

DOI: https://doi.org/10.5281/zenodo.18845124

ABSTRACT:

ಡಿಜಿಟಲ್ ಕ್ರಾಂತಿಯು ಭಾರತದ ಸಾಮಾಜಿಕ-ಆರ್ಥಿಕ ಸ್ವರೂಪವನ್ನು ಮೂಲಭೂತವಾಗಿ ಬದಲಾಯಿಸಿದೆ, ವ್ಯವಹಾರಗಳು ಮತ್ತು ಸಂವಹನಗಳನ್ನು ಭೌತಿಕ ಸ್ಥಳಗಳಿಂದ ವರ್ಚುವಲ್ ಜಗತ್ತಿಗೆ ವರ್ಗಾಯಿಸಿದೆ. ಈ ಬದಲಾವಣೆಯು ಎಲೆಕ್ಟ್ರಾನಿಕ್ ವಾಣಿಜ್ಯ, ಡಿಜಿಟಲ್ ಸಹಿಗಳು ಮತ್ತು ಹೆಚ್ಚುತ್ತಿರುವ ಸೈಬರ್ ಅಪರಾಧಗಳನ್ನು ನಿಯಂತ್ರಿಸಲು ಬಲವಾದ ಕಾನೂನು ಚೌಕಟ್ಟನ್ನು ಅನಿವಾರ್ಯವಾಗಿಸಿದೆ. ಈ ಪ್ರಬಂಧವು ಭಾರತದಲ್ಲಿ ಸೈಬರ್ ಕಾನೂನಿನ ವಿಕಸನವನ್ನು ಸಮಗ್ರವಾಗಿ ವಿಶ್ಲೇಷಿಸುತ್ತದೆ, ಮುಖ್ಯವಾಗಿ ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ (IT) ಕಾಯ್ದೆ 2000 ಮತ್ತು ಅದರ 2008ರ ತಿದ್ದುಪಡಿಗಳ ಮೇಲೆ ಕೇಂದ್ರೀಕರಿಸುತ್ತದೆ. ಇದಲ್ಲದೆ, ಡಿಜಿಟಲ್ ವೈಯಕ್ತಿಕ ದತ್ತಾಂಶ ಸಂರಕ್ಷಣಾ (DPDP) ಕಾಯ್ದೆ 2023ರ ಪರಿಣಾಮಕಾರಿ ಪ್ರಭಾವ ಮತ್ತು ಕೃತಕ ಬುದ್ಧಿಮತ್ತೆ (AI) ಹಾಗೂ ಡೀಪ್‌ಫೇಕ್‌ಗಳಿಂದ ಉಂಟಾಗುತ್ತಿರುವ ಸವಾಲುಗಳನ್ನು ಇದು ಪರಿಶೀಲಿಸುತ್ತದೆ. ನ್ಯಾಯಾಂಗ ವ್ಯಾಖ್ಯಾನಗಳ ಜೊತೆಗೆ ಕಾನೂನು ನಿಬಂಧನೆಗಳನ್ನು ಮೌಲ್ಯಮಾಪನ ಮಾಡುವ ಮೂಲಕ, ಈ ಅಧ್ಯಯನವು ಕಾನೂನು ತಂತ್ರಜ್ಞಾನ-ಕೇಂದ್ರಿತದಿಂದ ಹಕ್ಕು-ಆಧಾರಿತ ಚೌಕಟ್ಟಿನತ್ತ ಹೇಗೆ ಬದಲಾಗಿದೆ ಎಂಬುದನ್ನು ಎತ್ತಿ ತೋರಿಸುತ್ತದೆ. ಭಾರತವು ಡಿಜಿಟಲ್ ಶಾಸನದಲ್ಲಿ ಗಮನಾರ್ಹ ಪ್ರಗತಿಯನ್ನು ಸಾಧಿಸಿದ್ದರೂ, ಪ್ರಸ್ತುತ ಡಿಜಿಟಲ್ ವ್ಯವಸ್ಥೆಯ ಸಂಕೀರ್ಣತೆಗಳನ್ನು ಎದುರಿಸಲು ಕ್ರಿಯಾತ್ಮಕ ಮತ್ತು ವಿಶೇಷ ಸೈಬರ್ ಭದ್ರತಾ ಕಾನೂನು ಅತ್ಯಗತ್ಯ ಎಂದು ಈ ಅಧ್ಯಯನವು ತೀರ್ಮಾನಿಸುತ್ತದೆ.

KEYWORDS:

ಸೈಬರ್ ಕಾನೂನು, ಐಟಿ ಕಾಯ್ದೆ 2000, ಡಿಪಿಡಿಪಿ ಕಾಯ್ದೆ 2023, ಸೈಬರ್ ಭದ್ರತೆ, ಡಿಜಿಟಲ್ ಸಹಿಗಳು, ಸೈಬರ್ ಅಪರಾಧ.

ಪೀಠಿಕೆ:

ಭಾರತವು ಟ್ರಿಲಿಯನ್ ಡಾಲರ್ ಡಿಜಿಟಲ್ ಆರ್ಥಿಕತೆಯತ್ತ ಸಾಗುತ್ತಿರುವಂತೆ, ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನದ ಮೇಲಿನ ಅವಲಂಬನೆಯು ಕೇವಲ ಸಂವಹನವನ್ನು ಮೀರಿ ನಿರ್ಣಾಯಕ ಮೂಲಸೌಕರ್ಯ, ಆಡಳಿತ ಮತ್ತು ದೈನಂದಿನ ವಾಣಿಜ್ಯವನ್ನು ಒಳಗೊಂಡಿದೆ. ಆದಾಗ್ಯೂ, ಇಂಟರ್ನೆಟ್‌ನ ಗಡಿಯಿಲ್ಲದ ಮತ್ತು ಅನಾಮಧೇಯ ಸ್ವರೂಪವು "ಮುಖವಿಲ್ಲದ" ಅಪರಾಧಗಳ ಹೊಸ ವರ್ಗಕ್ಕೆ ಜನ್ಮ ನೀಡಿದೆ. ಸೈಬರ್ ಕಾನೂನು ಈ ಡಿಜಿಟಲ್ ಗಡಿಯನ್ನು ನಿಯಂತ್ರಿಸುವ ಮೂಲಸೌಕರ್ಯವಾಗಿ ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತದೆ.

ಭಾರತದಲ್ಲಿ, ಕಾನೂನು ಪಯಣವು 2000 ರಲ್ಲಿ ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯ್ದೆಯ ಜಾರಿಯೊಂದಿಗೆ ಪ್ರಾರಂಭವಾಯಿತು. ಎಲೆಕ್ಟ್ರಾನಿಕ್ ವಾಣಿಜ್ಯದ ಮೇಲಿನ UNCITRAL ಮಾದರಿ ಕಾನೂನನ್ನು ಆಧರಿಸಿ ಇದನ್ನು ರೂಪಿಸಲಾಯಿತು. ಆದರೂ, ಹ್ಯಾಕಿಂಗ್‌ನಿಂದ ಹಿಡಿದು ಸಂಕೀರ್ಣ AI-ಚಾಲಿತ ವಂಚನೆಗಳವರೆಗೆ ತಂತ್ರಜ್ಞಾನದ ಕ್ಷಿಪ್ರ ಬದಲಾವಣೆಗಳು ಈ ಶಾಸನದ ಮಿತಿಗಳನ್ನು ನಿರಂತರವಾಗಿ ಪರೀಕ್ಷಿಸಿವೆ. ಇಂದು, ಭಾರತದಲ್ಲಿ ಸೈಬರ್ ಕಾನೂನಿನ ಚರ್ಚೆಯು ಕೇವಲ ಅನಧಿಕೃತ ಪ್ರವೇಶವನ್ನು ದಂಡಿಸುವುದಕ್ಕೆ ಸೀಮಿತವಾಗಿಲ್ಲ; ಇದು ಜಾಗತಿಕ ಅಂತರ್-ಸಂಪರ್ಕದ ಯುಗದಲ್ಲಿ ದತ್ತಾಂಶ ಸಾರ್ವಭೌಮತ್ವ, ವೈಯಕ್ತಿಕ ಗೌಪ್ಯತೆ ಮತ್ತು ರಾಷ್ಟ್ರೀಯ ಭದ್ರತೆಯ ಬಗ್ಗೆಯೂ ಚರ್ಚಿಸುತ್ತದೆ.

ಗುರಿ ಮತ್ತು ಉದ್ದೇಶಗಳು:

ಗುರಿಗಳು:

ಭಾರತದಲ್ಲಿ ಅಸ್ತಿತ್ವದಲ್ಲಿರುವ ಸೈಬರ್ ಕಾನೂನು ಚೌಕಟ್ಟಿನ ಪರಿಣಾಮಕಾರಿತ್ವವನ್ನು ಮೌಲ್ಯಮಾಪನ ಮಾಡುವುದು ಮತ್ತು ಉದಯೋನ್ಮುಖ ತಂತ್ರಜ್ಞಾನಗಳಿಂದ ಉಂಟಾಗುವ ಶಾಸಕಾಂಗದ ಅಂತರವನ್ನು ಗುರುತಿಸುವುದು ಈ ಸಂಶೋಧನೆಯ ಪ್ರಾಥಮಿಕ ಗುರಿಯಾಗಿದೆ.

ಉದ್ದೇಶಗಳು:

- ಐಟಿ ಕಾಯ್ದೆ 2000ರ ಐತಿಹಾಸಿಕ ವಿಕಸನ ಮತ್ತು 2008ರ ತಿದ್ದುಪಡಿಗಳ ಪ್ರಾಮುಖ್ಯತೆಯನ್ನು ಪತ್ತೆಹಚ್ಚುವುದು.
- ಸೈಬರ್ ಅಪರಾಧಗಳಿಗೆ ಸಂಬಂಧಿಸಿದ ಪ್ರಮುಖ ನಿಬಂಧನೆಗಳು ಮತ್ತು ಎಲೆಕ್ಟ್ರಾನಿಕ್ ದಾಖಲೆಗಳ ಕಾನೂನು ಮಾನ್ಯತೆಯನ್ನು ವಿಶ್ಲೇಷಿಸುವುದು.
- ಕಾರ್ಪೊರೇಟ್ ಮತ್ತು ವೈಯಕ್ತಿಕ ದತ್ತಾಂಶ ನಿರ್ವಹಣೆಯ ಮೇಲೆ ಡಿಜಿಟಲ್ ವೈಯಕ್ತಿಕ ದತ್ತಾಂಶ ಸಂರಕ್ಷಣಾ ಕಾಯ್ದೆ, 2023 ರ ಪ್ರಭಾವವನ್ನು ಪರಿಶೀಲಿಸುವುದು.
- 2026 ರಲ್ಲಿ AI, ಡೀಪ್‌ಫೇಕ್‌ಗಳು ಮತ್ತು ದೇಶೀಯ ಗಡಿಯಾಚೆಗಿನ ಕಾನೂನು ವ್ಯಾಪ್ತಿಯ ಸಮಸ್ಯೆಗಳಿಂದ ಉಂಟಾಗುವ ಪ್ರಸ್ತುತ ಸವಾಲುಗಳನ್ನು ಗುರುತಿಸುವುದು.

ಅಧ್ಯಯನದ ವ್ಯಾಪ್ತಿ:

ಈ ಪ್ರಬಂಧವು 2000ರ ಐಟಿ ಕಾಯ್ದೆಯ ಪ್ರಾರಂಭದಿಂದ 2026ರ ಸಮಕಾಲೀನ ನಿಯಂತ್ರಕ ಪರಿಸರದವರೆಗಿನ ಶಾಸಕಾಂಗ ಬೆಳವಣಿಗೆಗಳನ್ನು ಒಳಗೊಂಡಿದೆ. ಇದು ಭಾರತೀಯ ನ್ಯಾಯವ್ಯಾಪ್ತಿಯಲ್ಲಿನ ಕ್ರಿಮಿನಲ್ ನಿಬಂಧನೆಗಳು, ಮಧ್ಯವರ್ತಿಗಳ ಹೊಣೆಗಾರಿಕೆಗಳು ಮತ್ತು ದತ್ತಾಂಶ ಸಂರಕ್ಷಣಾ ಮಾನದಂಡಗಳ ಮೇಲೆ ಕೇಂದ್ರೀಕರಿಸುತ್ತದೆ. ಮೂಲ ವಿಶ್ಲೇಷಣೆಯು ಭಾರತೀಯ ಶಾಸನಗಳು ಮತ್ತು ಸುಪ್ರೀಂ ಕೋರ್ಟ್ ನಿದರ್ಶನಗಳ

ಮೇಲೆ ಕೇಂದ್ರೀಕೃತವಾಗಿದೆ.

ಸಂಶೋಧನಾ ವಿಧಾನ:

ಈ ಸಂಶೋಧನೆಯು ಕೇವಲ ದ್ವಿತೀಯಕ ದತ್ತಾಂಶವನ್ನು (Secondary Data) ಬಳಸಿಕೊಂಡು ಸೈದ್ಧಾಂತಿಕ ಸಂಶೋಧನಾ ವಿಧಾನವನ್ನು (Doctrinal Research Methodology) ಆಧರಿಸಿದೆ. ಈ ಅಧ್ಯಯನವು ಶಾಸನಬದ್ಧ ನಿಬಂಧನೆಗಳು (ಐಟಿ ಕಾಯ್ದೆ, ಡಿಪಿಡಿಪಿ ಕಾಯ್ದೆ), ನ್ಯಾಯಾಂಗ ತೀರ್ಪುಗಳು, ಸಂಸದೀಯ ವರದಿಗಳು ಮತ್ತು ವಿದ್ವತ್ಪೂರ್ಣ ಲೇಖನಗಳ ವ್ಯವಸ್ಥಿತ ವಿಶ್ಲೇಷಣೆಯನ್ನು ಒಳಗೊಂಡಿದೆ. ಪ್ರಸ್ತುತ ಭಾರತೀಯ ಸೈಬರ್-ನಿಯಂತ್ರಕ ಚೌಕಟ್ಟಿನಲ್ಲಿನ ಪ್ರವೃತ್ತಿಗಳು ಮತ್ತು ಕಾನೂನು ಅಂತರವನ್ನು ಗುರುತಿಸಲು ದತ್ತಾಂಶವನ್ನು ಸಂಶ್ಲೇಷಿಸಲಾಗಿದೆ.

ಐತಿಹಾಸಿಕ ಹಿನ್ನೆಲೆ ಮತ್ತು ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯ್ದೆ, 2000:

ಐತಿಹಾಸಿಕ ಹಿನ್ನೆಲೆ:

ಭಾರತದಲ್ಲಿ ಸೈಬರ್ ಕಾನೂನಿನ ಉಗಮವು ಕೇವಲ ಆಂತರಿಕ ಅಗತ್ಯವಾಗಿರಲಿಲ್ಲ, ಬದಲಿಗೆ ಜಾಗತಿಕ ಬದಲಾವಣೆಯ ಪ್ರತಿಫಲವಾಗಿತ್ತು. UNCITRAL (United Nations Commission on International Trade Law) ಮಾದರಿ ಕಾನೂನು ಭಾರತದ ಸೈಬರ್ ಕಾನೂನಿನ 'ಜನನಿ' ಇದ್ದಂತೆ. 1996ರಲ್ಲಿ ಅಂಗೀಕರಿಸಲ್ಪಟ್ಟ ಈ ಮಾದರಿಯು ಜಾಗತಿಕವಾಗಿ ಡಿಜಿಟಲ್ ವ್ಯವಹಾರಗಳಿಗೆ ಒಂದು ಏಕರೂಪದ ಚೌಕಟ್ಟನ್ನು ನೀಡಿತು.

UNCITRAL ಮಾದರಿ ಕಾನೂನು (1996): ಸೈಬರ್ ಕಾನೂನಿನ ಜಾಗತಿಕ ಅಡಿಪಾಯ

ವಿಶ್ವಸಂಸ್ಥೆಯು ಅಂತರರಾಷ್ಟ್ರೀಯ ವ್ಯಾಪಾರದಲ್ಲಿ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಸಂವಹನಗಳ ಬಳಕೆಯನ್ನು ಸುಗಮಗೊಳಿಸಲು ಈ ಮಾದರಿ ಕಾನೂನನ್ನು ರೂಪಿಸಿತು. ಭಾರತವು ಈ ಮಾದರಿಯನ್ನು ಆಧರಿಸಿ ತನ್ನ ಐಟಿ ಕಾಯ್ದೆಯನ್ನು ರೂಪಿಸಿದ್ದು, ಇದರ ಪ್ರಮುಖ ವೈಶಿಷ್ಟ್ಯಗಳು ಈ ಕೆಳಗಿನಂತಿವೆ:

1. "ಕ್ರಿಯಾತ್ಮಕ ಸಮಾನತೆ"ಯ ತತ್ವ

UNCITRAL ಮಾದರಿಯ ಅತ್ಯಂತ ಪ್ರಮುಖ ಕೊಡುಗೆ ಎಂದರೆ ಈ ತತ್ವ. ಇದು ಹೇಳುವುದೇನೆಂದರೆ: "ಒಂದು ಕಾಗದದ ದಾಖಲೆಯು ಯಾವ ಕಾನೂನುಬದ್ಧ ಕಾರ್ಯವನ್ನು ನಿರ್ವಹಿಸುತ್ತದೆಯೋ (ಉದಾಹರಣೆಗೆ ಸಾಕ್ಷ್ಯ ನೀಡುವುದು ಅಥವಾ ಸಹಿ ಹಾಕುವುದು), ಅದೇ ಕಾರ್ಯವನ್ನು ಎಲೆಕ್ಟ್ರಾನಿಕ್ ದಾಖಲೆಯೂ ನಿರ್ವಹಿಸಿದರೆ, ಅದನ್ನು ಕಾನೂನುಬದ್ಧವಾಗಿ ಕಾಗದಕ್ಕೆ ಸಮಾನ ಎಂದು ಪರಿಗಣಿಸಬೇಕು." ಭಾರತದ ಐಟಿ ಕಾಯ್ದೆಯ ಸೆಕ್ಷನ್ 4 ಮತ್ತು 5 ಈ ತತ್ವದ ಮೇಲೆ ನೇರವಾಗಿ ಆಧಾರಿತವಾಗಿದೆ.

2. ತಾಂತ್ರಿಕ ತಟಸ್ಥತೆ

UNCITRAL ಮಾದರಿಯು ಯಾವುದೇ ಒಂದು ನಿರ್ದಿಷ್ಟ ತಂತ್ರಜ್ಞಾನಕ್ಕೆ (ಉದಾಹರಣೆಗೆ ಒಂದು ನಿರ್ದಿಷ್ಟ ಸಾಫ್ಟ್‌ವೇರ್ ಅಥವಾ ಕಂಪನಿ) ಸೀಮಿತವಾಗಿರಬಾರದು ಎಂದು ಪ್ರತಿಪಾದಿಸಿತು. ಕಾನೂನು ತಂತ್ರಜ್ಞಾನಕ್ಕಿಂತ ಮಿಗಿಲಾಗಿರಬೇಕು, ಇದರಿಂದ ತಂತ್ರಜ್ಞಾನ ಬದಲಾದರೂ ಕಾನೂನು ಬದಲಾಗುವ ಅಗತ್ಯವಿರುವುದಿಲ್ಲ.

3. ಇ-ಕಾಮರ್ಸ್‌ಗೆ ಅಂತರರಾಷ್ಟ್ರೀಯ ಮಾನ್ಯತೆ

ಪ್ರತಿಯೊಂದು ದೇಶವೂ ತನ್ನದೇ ಆದ ವಿಭಿನ್ನ ನಿಯಮಗಳನ್ನು ಹೊಂದಿದ್ದರೆ ಜಾಗತಿಕ ಇ-ಕಾಮರ್ಸ್ ಕಷ್ಟವಾಗುತ್ತದೆ. UNCITRAL ಮಾದರಿಯು ಎಲ್ಲ ದೇಶಗಳಿಗೂ ಒಂದೇ ರೀತಿಯ ಕಾನೂನು ಚೌಕಟ್ಟನ್ನು ನೀಡಿತು. ಭಾರತವು ಇದನ್ನು ಅಳವಡಿಸಿಕೊಂಡಿದ್ದರಿಂದ, ವಿದೇಶಿ ಕಂಪನಿಗಳಿಗೆ ಭಾರತದಲ್ಲಿ ಡಿಜಿಟಲ್ ವ್ಯವಹಾರ ಮಾಡಲು ಕಾನೂನುಬದ್ಧ ಭರವಸೆ ಸಿಕ್ಕಂತಾಯಿತು.

4. ಕಾನೂನು ಮಾನ್ಯತೆಯ ನಾಲ್ಕು ಸ್ತಂಭಗಳು

UNCITRAL ಮಾದರಿಯು ಈ ಕೆಳಗಿನವುಗಳಿಗೆ ಕಾನೂನು ಮಾನ್ಯತೆ ನೀಡಲು ಶಿಫಾರಸು ಮಾಡಿತು:

- ಬರವಣಿಗೆ (Writing): ಡಿಜಿಟಲ್ ರೂಪದ ಬರವಣಿಗೆಯೂ ಮಾನ್ಯ.
- ಸಹಿ (Signature): ಡಿಜಿಟಲ್ ಸಹಿಗಳು ಹಸ್ತಚಾಲಿತ ಸಹಿಗಳಿಗೆ ಸಮಾನ.
- ಮೂಲ ದಾಖಲೆ (Original): ಡಿಜಿಟಲ್ ಫೈಲ್‌ಗಳನ್ನು 'ಮೂಲ ಪ್ರತಿ' ಎಂದು ಒಪ್ಪಿಕೊಳ್ಳಬಹುದು.
- ದಾಖಲೆಗಳ ಸಂಗ್ರಹ (Retention): ಕಾಗದದ ಫೈಲ್‌ಗಳ ಬದಲಿಗೆ ಸರ್ವರ್‌ಗಳಲ್ಲಿ ಮಾಹಿತಿ ಉಳಿಸುವುದು ಕಾನೂನುಬದ್ಧ.

ಭಾರತವು ಈ ಮಾದರಿ ಕಾನೂನನ್ನು ಅಳವಡಿಸಿಕೊಂಡ 12ನೇ ದೇಶವಾಗಿದೆ. 30 ಜನವರಿ 1997ರಂದು ವಿಶ್ವಸಂಸ್ಥೆಯ ಸಾಮಾನ್ಯ ಸಭೆಯು (General Assembly) ಸದಸ್ಯ ರಾಷ್ಟ್ರಗಳು ತಮ್ಮ ದೇಶದ ಕಾನೂನುಗಳನ್ನು ಈ ಮಾದರಿಗೆ ಅನುಗುಣವಾಗಿ ಬದಲಿಸಿಕೊಳ್ಳುವಂತೆ ಶಿಫಾರಸು ಮಾಡಿತು. ಈ ಕರೆಗೆ ಓಗೊಟ್ಟು ಭಾರತವು Information Technology Bill, 1999 ಅನ್ನು ಮಂಡಿಸಿ, ನಂತರ ಅದು 17 ಮೇ 2000ರಂದು ಐಟಿ ಕಾಯ್ದೆಯನ್ನು ಸಂಸತ್ತಿನಲ್ಲಿ ಅಂಗೀಕರಿಸಲಾಯಿತು ಮತ್ತು 17 ಅಕ್ಟೋಬರ್ 2000 ರಂದು ಇದು ಜಾರಿಗೆ ಬಂದಿತು. ನಂತರ IT Act, 2000 ಆಗಿ ಜಾರಿಗೆ ಬಂದಿತು.

ಐಟಿ ಕಾಯ್ದೆ 2000 ರ ಮೂಲ ಉದ್ದೇಶಗಳು

ಈ ಕಾಯ್ದೆಯನ್ನು ಮುಖ್ಯವಾಗಿ ನಾಲ್ಕು ಆಧಾರಸ್ತಂಭಗಳ ಮೇಲೆ ನಿರ್ಮಿಸಲಾಗಿದೆ:

- ಎಲೆಕ್ಟ್ರಾನಿಕ್ ವ್ಯವಹಾರಗಳಿಗೆ ಮಾನ್ಯತೆ: ಇ-ಕಾಮರ್ಸ್ ಮೂಲಕ ನಡೆಯುವ ಒಪ್ಪಂದಗಳಿಗೆ ಕಾನೂನುಬದ್ಧ ಮಾನ್ಯತೆ ನೀಡುವುದು.
- ಡಿಜಿಟಲ್ ಸಹಿ (Digital Signatures): ಆನ್‌ಲೈನ್ ದಾಖಲೆಗಳನ್ನು ದೃಢೀಕರಿಸಲು ಡಿಜಿಟಲ್ ಸಹಿಗಳನ್ನು ಕಾನೂನುಬದ್ಧಗೊಳಿಸುವುದು.
- ಇ-ಗವರ್ನನ್ಸ್ (e-Governance): ಸರ್ಕಾರಿ ಕಚೇರಿಗಳಲ್ಲಿ ದಾಖಲೆಗಳನ್ನು ಎಲೆಕ್ಟ್ರಾನಿಕ್ ರೂಪದಲ್ಲಿ ಸಲ್ಲಿಸಲು ಮತ್ತು ಸಂಗ್ರಹಿಸಲು ದಾರಿ ಮಾಡಿಕೊಡುವುದು.
- ಸೈಬರ್ ಅಪರಾಧಗಳ ನಿಯಂತ್ರಣ: ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆಗಳಿಗೆ ಹಾನಿ ಮಾಡುವುದು ಅಥವಾ ಅನಧಿಕೃತ ಪ್ರವೇಶ ಪಡೆಯುವುದನ್ನು ಅಪರಾಧವೆಂದು ಪರಿಗಣಿಸುವುದು.

2000ರ ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯ್ದೆಯ ಪ್ರಮುಖ ನಿಬಂಧನೆಗಳು (Key Sections)

ಈ ಕಾಯ್ದೆಯ ಈ ಕೆಳಗಿನ ಸೆಕ್ಷನ್‌ಗಳು ಅತ್ಯಂತ ನಿರ್ಣಾಯಕವಾಗಿವೆ:

- ಸೆಕ್ಷನ್ 43: ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ನೆಟ್‌ವರ್ಕ್‌ಗೆ ಹಾನಿ ಮಾಡಿದರೆ ಸಿವಿಲ್ ಹೊಣೆಗಾರಿಕೆ ಮತ್ತು ಪರಿಹಾರದ ಬಗ್ಗೆ ವಿವರಿಸುತ್ತದೆ.
- ಸೆಕ್ಷನ್ 65: ಕಂಪ್ಯೂಟರ್ ಸೋರ್ಸ್ ಕೋಡ್ ಅನ್ನು ತಿದ್ದುವುದಕ್ಕೆ ಸಂಬಂಧಿಸಿದ ಶಿಕ್ಷೆ.
- ಸೆಕ್ಷನ್ 66: ಹ್ಯಾಕಿಂಗ್ ಮತ್ತು ಕಂಪ್ಯೂಟರ್ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು.
- ಸೆಕ್ಷನ್ 67: ಇಂಟರ್ನೆಟ್‌ನಲ್ಲಿ ಅಶ್ಲೀಲ ಮಾಹಿತಿಯನ್ನು ಪ್ರಕಟಿಸುವುದಕ್ಕೆ ಸಂಬಂಧಿಸಿದ ನಿಬಂಧನೆಗಳು.
- ಸೆಕ್ಷನ್ 70: ನಿರ್ಣಾಯಕ ಮಾಹಿತಿ ಮೂಲಸೌಕರ್ಯಗಳಿಗೆ (Critical Information Infrastructure) ರಕ್ಷಣೆ ನೀಡುವುದು.

ನಿಯಂತ್ರಕ ವ್ಯವಸ್ಥೆ:

ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯ್ದೆ (2000)ಯು ಪ್ರಮಾಣೀಕರಿಸುವ ಅಧಿಕಾರಿಗಳ ನಿಯಂತ್ರಕ (Controller of Certifying Authorities – CCA) ಹುದ್ದೆಯನ್ನು ಸೃಷ್ಟಿಸಿತು. ಡಿಜಿಟಲ್ ಸಹಿಗಳನ್ನು ನೀಡುವ ಸಂಸ್ಥೆಗಳ ಮೇಲೆ ನಿಗಾ ಇಡುವುದು ಮತ್ತು ಪರವಾನಗಿ ನೀಡುವುದು ಇದರ ಕೆಲಸವಾಗಿದೆ. ಅಲ್ಲದೆ, ಸೈಬರ್ ಅಪರಾಧಗಳ ಮೇಲ್ಮನವಿಗಳನ್ನು ಆಲಿಸಲು 'ಸೈಬರ್ ಅಪೀಲೇಟ್ ಟ್ರಿಬ್ಯೂನಲ್' ಅನ್ನು ಸ್ಥಾಪಿಸಲಾಯಿತು.

2008 ರ ತಿದ್ದುಪಡಿ: ಬದಲಾದ ಕಾನೂನು ಚೌಕಟ್ಟು

2000ರಲ್ಲಿ ಜಾರಿಗೆ ಬಂದ ಮೂಲ ಕಾಯ್ದೆಯು ಮುಖ್ಯವಾಗಿ ಇ-ಕಾಮರ್ಸ್ ಮೇಲೆ ಕೇಂದ್ರೀಕರಿಸಿತ್ತು. ಆದರೆ, 2000 ಮತ್ತು 2008ರ ನಡುವೆ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮಗಳ ಬಳಕೆ, ಮೊಬೈಲ್ ಫೋನ್‌ಗಳ ಬಳಕೆ ಮತ್ತು ಸುಧಾರಿತ ಸೈಬರ್ ದಾಳಿಗಳು ಹೆಚ್ಚಾದವು. ಈ ಹಿನ್ನೆಲೆಯಲ್ಲಿ, 2008ರ ಡಿಸೆಂಬರ್‌ನಲ್ಲಿ ಸಂಸತ್ತು ಐಟಿ ತಿದ್ದುಪಡಿ ಕಾಯ್ದೆಯನ್ನು ಅಂಗೀಕರಿಸಿತು ಮತ್ತು ಇದು 27 ಅಕ್ಟೋಬರ್ 2009 ರಿಂದ ಜಾರಿಗೆ ಬಂದಿತು.

2008 ರ ತಿದ್ದುಪಡಿಯ ಪ್ರಮುಖ ಬದಲಾವಣೆಗಳು ಮತ್ತು ಸೇರ್ಪಡೆಗಳು

1. ತಂತ್ರಜ್ಞಾನ ತಟಸ್ಥತೆ:

ಮೂಲ ಕಾಯ್ದೆಯು ಕೇವಲ "ಡಿಜಿಟಲ್ ಸಹಿ" (Digital Signature) ಬಗ್ಗೆ ಮಾತನಾಡುತ್ತಿತ್ತು, ಇದು ನಿರ್ದಿಷ್ಟ ತಂತ್ರಜ್ಞಾನಕ್ಕೆ ಸೀಮಿತವಾಗಿತ್ತು. 2008ರ ತಿದ್ದುಪಡಿಯು ಇದನ್ನು "ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಸಹಿ" (Electronic Signature) ಎಂದು ಬದಲಾಯಿಸಿತು. ಇದರಿಂದಾಗಿ ಭವಿಷ್ಯದಲ್ಲಿ ಬರುವ ಯಾವುದೇ ಹೊಸ ದೃಢೀಕರಣ ತಂತ್ರಜ್ಞಾನವನ್ನು ಕಾನೂನಿನ ಅಡಿ ತರಲು ಸಾಧ್ಯವಾಯಿತು.

2. ಕಾರ್ಪೊರೇಟ್ ಹೊಣೆಗಾರಿಕೆ (ಸೆಕ್ಷನ್ 43A):

ಈ ತಿದ್ದುಪಡಿಯು ದತ್ತಾಂಶ ಸಂರಕ್ಷಣೆಯ ಜವಾಬ್ದಾರಿಯನ್ನು ಕಂಪನಿಗಳ ಮೇಲೆ ಹೇರಿತು. ಯಾವುದೇ ಸಂಸ್ಥೆಯು ತನ್ನ ಗ್ರಾಹಕರ ವೈಯಕ್ತಿಕ ದತ್ತಾಂಶವನ್ನು (Sensitive Personal Data) ಸುರಕ್ಷಿತವಾಗಿರಿಸಲು ವಿಫಲವಾದರೆ ಮತ್ತು ಅದರಿಂದ ಯಾರಿಗಾದರೂ ನಷ್ಟವಾದರೆ, ಆ ಸಂಸ್ಥೆಯು ಅಪರಿಮಿತ ಪರಿಹಾರವನ್ನು (Unlimited Compensation) ನೀಡಬೇಕೆಂದು ಈ ಸೆಕ್ಷನ್ ಹೇಳುತ್ತದೆ.

3. ಸೈಬರ್ ಭಯೋತ್ಪಾದನೆ (ಸೆಕ್ಷನ್ 66F):

ಸೈಬರ್ ಭಯೋತ್ಪಾದನೆ (ಸೆಕ್ಷನ್ 66F) ಇದು ದೇಶದ ಏಕತೆ, ಸಮಗ್ರತೆ, ಭದ್ರತೆ ಅಥವಾ ಸಾರ್ವಭೌಮತ್ವಕ್ಕೆ ಧಕ್ಕೆ ತರುವ ಅಥವಾ ಜನರ ನಡುವೆ ಭಯ ಹುಟ್ಟಿಸುವ ಉದ್ದೇಶದಿಂದ ಕಂಪ್ಯೂಟರ್ ಸಂಪನ್ಮೂಲಗಳ ಮೇಲೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಹಾನಿಕಾರಕ ಸಾಫ್ಟ್‌ವೇರ್ ಪರಿಚಯಿಸುವುದು, ಅಥವಾ ದೇಶದ ರಕ್ಷಣಾ ವ್ಯವಸ್ಥೆಗಳು, ನಿರ್ಣಾಯಕ ಮೂಲಸೌಕರ್ಯಗಳಂತಹವುಗಳ ಮೇಲೆ ದಾಳಿ ಮಾಡುವುದನ್ನು ವಿವರಿಸುತ್ತದೆ. ಈ ಅಪರಾಧಕ್ಕೆ ಜೀವಾವಧಿ ಶಿಕ್ಷೆಯವರೆಗೆ ಶಿಕ್ಷೆ ವಿಧಿಸಬಹುದು ಮತ್ತು ಇದು ಅತ್ಯಂತ ಗಂಭೀರವಾದ ಸೈಬರ್ ಅಪರಾಧವಾಗಿದೆ.

4. ಹೊಸ ಸೈಬರ್ ಅಪರಾಧಗಳ ವ್ಯಾಖ್ಯಾನ:

ತಂತ್ರಜ್ಞಾನದ ದುರುಪಯೋಗವನ್ನು ತಡೆಯಲು ಈ ಕೆಳಗಿನ ಹೊಸ ಸೆಕ್ಷನ್‌ಗಳನ್ನು ಸೇರಿಸಲಾಯಿತು:

- ಸೆಕ್ಷನ್ 66B: ಕಳ್ಳತನ ಮಾಡಿದ ಕಂಪ್ಯೂಟರ್ ಸಂಪನ್ಮೂಲಗಳನ್ನು ಸ್ವೀಕರಿಸುವುದು.
- ಸೆಕ್ಷನ್ 66C: ಗುರುತಿನ ಕಳ್ಳತನ (Identity Theft) – ಅಂದರೆ ಬೇರೆಯವರ ಪಾಸ್‌ವರ್ಡ್ ಅಥವಾ ಡಿಜಿಟಲ್ ಸಹಿ ಬಳಸುವುದು.
- ಸೆಕ್ಷನ್ 66D: ಕಂಪ್ಯೂಟರ್ ಬಳಸಿ ವೇಷ ಮರೆಸಿ ವಂಚಿಸುವುದು (Cheating by Personation).
- ಸೆಕ್ಷನ್ 66E: ವೈಯಕ್ತಿಕ ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆ (Privacy Violation) – ಅನುಮತಿಯಿಲ್ಲದೆ ಖಾಸಗಿ ದೃಶ್ಯಗಳನ್ನು ಚಿತ್ರೀಕರಿಸುವುದು ಅಥವಾ ಪ್ರಕಟಿಸುವುದು.

5. ಮಧ್ಯವರ್ತಿಗಳ ಹೊಣೆಗಾರಿಕೆ (ಸೆಕ್ಷನ್ 79):

ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಮತ್ತು ಇಂಟರ್ನೆಟ್ ಸೇವೆ ಒದಗಿಸುವ ಸಂಸ್ಥೆಗಳಿಗೆ (Intermediaries) 'ಸೇಫ್ ಹಾರ್ಬರ್' (Safe Harbor) ರಕ್ಷಣೆಯನ್ನು ಈ ತಿದ್ದುಪಡಿಯು ಸ್ಪಷ್ಟಪಡಿಸಿತು. ಅಂದರೆ, ಈ ವೇದಿಕೆಗಳಲ್ಲಿ ಬಳಕೆದಾರರು ಹಾಕುವ ಮಾಹಿತಿಗೆ ಸಂಸ್ಥೆಗಳು ಜವಾಬ್ದಾರರಲ್ಲ, ಆದರೆ ಸರ್ಕಾರ ಸೂಚಿಸಿದಾಗ ಅಂತಹ ಕಾನೂನುಬಾಹಿರ ಮಾಹಿತಿಯನ್ನು ತೆಗೆದುಹಾಕುವ ಜವಾಬ್ದಾರಿ ಅವರದ್ದಾಗಿರುತ್ತದೆ.

6. ವಿವಾದಾತ್ಮಕ ಸೆಕ್ಷನ್ 66A

ಈ ತಿದ್ದುಪಡಿಯ ಮೂಲಕ 'ಸೆಕ್ಷನ್ 66A' ಅನ್ನು ಪರಿಚಯಿಸಲಾಯಿತು, ಇದು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ "ಆಕ್ಷೇಪಾರ್ಹ" ಸಂದೇಶಗಳನ್ನು ಕಳುಹಿಸುವುದನ್ನು ಅಪರಾಧವೆಂದು ಪರಿಗಣಿಸಿತ್ತು. ನಂತರದ ದಿನಗಳಲ್ಲಿ ಇದು ವಾಕ್ ಸ್ವಾತಂತ್ರ್ಯದ ಮೇಲೆ ದಾಳಿ ಎಂದು ವಿವಾದಕ್ಕೀಡಾಯಿತು ಮತ್ತು 2015 ರಲ್ಲಿ ಸುಪ್ರೀಂ ಕೋರ್ಟ್ ಈ ಸೆಕ್ಷನ್ ಅನ್ನು ರದ್ದುಗೊಳಿಸಿತು.

2008ರ ತಿದ್ದುಪಡಿಯು ಭಾರತದ ಸೈಬರ್ ಕಾನೂನನ್ನು ಕೇವಲ "ವ್ಯಾಪಾರ ಕಾನೂನು" ಎಂಬ ಹಂತದಿಂದ "ಸಂಪೂರ್ಣ ಕ್ರಿಮಿನಲ್ ಮತ್ತು ನಾಗರಿಕ ಕಾನೂನು" ಎಂಬ ಹಂತಕ್ಕೆ ಏರಿಸಿತು. ಇದು ಇಂದಿನ ಆಧುನಿಕ ಸೈಬರ್ ಕಾನೂನು ವ್ಯವಸ್ಥೆಗೆ ಅಡಿಪಾಯ ಹಾಕಿಕೊಟ್ಟಿತು.

2023ರ ಡಿಜಿಟಲ್ ವೈಯಕ್ತಿಕ ದತ್ತಾಂಶ ಸಂರಕ್ಷಣಾ ಕಾಯ್ದೆ (Digital Personal

Data Protection–DPDP):

ದಶಕಗಳ ಕಾಲ ಭಾರತವು ದತ್ತಾಂಶ ಸಂರಕ್ಷಣೆಗಾಗಿ ಐಟಿ ಕಾಯ್ದೆಯ ಸೆಕ್ಷನ್ 43A ಮೇಲೆ ಅವಲಂಬಿತವಾಗಿತ್ತು. ಆದರೆ, 2017ರ ಪುಟ್ಟಸ್ವಾಮಿ ತೀರ್ಪಿನ ನಂತರ ಗೌಪ್ಯತೆ (Privacy) ಮೂಲಭೂತ ಹಕ್ಕಾದ ಹಿನ್ನೆಲೆಯಲ್ಲಿ, ಈ ಸಮಗ್ರ ಕಾನೂನನ್ನು 2023ರಲ್ಲಿ ಜಾರಿಗೆ ತರಲಾಯಿತು. ಇದು ಕೇವಲ ಅಪರಾಧ ತಡೆಯುವುದಲ್ಲದೆ, ದತ್ತಾಂಶದ ಮೇಲಿನ ವ್ಯಕ್ತಿಯ ಮಾಲೀಕತ್ವವನ್ನು ಎತ್ತಿಹಿಡಿಯುತ್ತದೆ.

DPDP ಕಾಯ್ದೆಯ ಪ್ರಮುಖ ಪಾರಿಭಾಷಿಕ ಪದಗಳು

ಸಂಶೋಧನಾ ದೃಷ್ಟಿಯಿಂದ ಈ ಮೂರು ಪದಗಳು ಅತ್ಯಂತ ಮುಖ್ಯ:

- ದತ್ತಾಂಶ ಪ್ರಿನ್ಸಿಪಾಲ್ (Data Principal): ಯಾವ ವ್ಯಕ್ತಿಯ ದತ್ತಾಂಶವನ್ನು ಸಂಗ್ರಹಿಸಲಾಗುತ್ತದೆಯೋ ಆ ವ್ಯಕ್ತಿ (ನಾಗರಿಕ).
- ದತ್ತಾಂಶ ಫಿಡುಷಿಯರಿ (Data Fiduciary): ದತ್ತಾಂಶವನ್ನು ಸಂಗ್ರಹಿಸುವ ಮತ್ತು ಅದರ ಬಳಕೆಯನ್ನು ನಿರ್ಧರಿಸುವ ಸಂಸ್ಥೆ (ಉದಾಹರಣೆಗೆ: ಬ್ಯಾಂಕ್, ಈ–ಕಾಮರ್ಸ್ ಸಂಸ್ಥೆ ಅಥವಾ ಸರ್ಕಾರ).
- ದತ್ತಾಂಶ ಪ್ರೊಸೆಸರ್ (Data Processor): ಫಿಡುಷಿಯರಿ ಪರವಾಗಿ ದತ್ತಾಂಶವನ್ನು ಸಂಸ್ಕರಿಸುವ ಹೊರಗಿನ ಏಜೆನ್ಸಿ.

ನಾಗರಿಕರ ಹಕ್ಕುಗಳು:

2023ರ DPDP ಕಾಯ್ದೆಯು ಭಾರತೀಯ ನಾಗರಿಕರಿಗೆ ನಾಲ್ಕು ಪ್ರಮುಖ ಹಕ್ಕುಗಳನ್ನು ನೀಡಿದೆ:

- ಮಾಹಿತಿ ಪಡೆಯುವ ಹಕ್ಕು: ತನ್ನ ದತ್ತಾಂಶವನ್ನು ಹೇಗೆ ಬಳಸಲಾಗುತ್ತಿದೆ ಎಂದು ತಿಳಿಯುವ ಹಕ್ಕು.
- ತಿದ್ದುಪಡಿ ಮತ್ತು ಅಳಿಸುವಿಕೆಯ ಹಕ್ಕು (Right to Erasure): ತಪ್ಪು ಮಾಹಿತಿಯನ್ನು ಸರಿಪಡಿಸುವ ಅಥವಾ ಇನ್ನು ಮುಂದೆ ಅಗತ್ಯವಿಲ್ಲದ ದತ್ತಾಂಶವನ್ನು ಅಳಿಸಿಹಾಕುವಂತೆ ಕೋರುವ ಹಕ್ಕು.
- ಕುಂದುಕೊರತೆ ನಿವಾರಣೆ: ದತ್ತಾಂಶ ದುರುಪಯೋಗವಾದರೆ ದೂರು ನೀಡುವ ಹಕ್ಕು.
- ನಾಮನಿರ್ದೇಶನ ಹಕ್ಕು: ತನ್ನ ಮರಣದ ನಂತರ ಅಥವಾ ಅಶಕ್ತತೆಯ ಸಂದರ್ಭದಲ್ಲಿ ದತ್ತಾಂಶ ನಿರ್ವಹಿಸಲು ಒಬ್ಬರನ್ನು ನಾಮನಿರ್ದೇಶನ ಮಾಡುವ ಹಕ್ಕು.

ದತ್ತಾಂಶ ಫಿಡುಷಿಯರಿಗಳ (Data Fiduciary) ಜವಾಬ್ದಾರಿಗಳು:

ಸಂಸ್ಥೆಗಳು ದತ್ತಾಂಶವನ್ನು ನಿರ್ವಹಿಸುವಾಗ ಈ ಕೆಳಗಿನ ನಿಯಮಗಳನ್ನು ಪಾಲಿಸುವುದು ಕಡ್ಡಾಯ:

- ಸ್ಪಷ್ಟ ಸಮ್ಮತಿ (Informed Consent): ದತ್ತಾಂಶ ಸಂಗ್ರಹಿಸುವ ಮೊದಲು ವ್ಯಕ್ತಿಯಿಂದ ಸರಳ ಮತ್ತು ಸ್ಪಷ್ಟ ಭಾಷೆಯಲ್ಲಿ ಸಮ್ಮತಿ ಪಡೆಯಬೇಕು.
- ದತ್ತಾಂಶ ಕನಿಷ್ಠೀಕರಣ: ಕೆಲಸಕ್ಕೆ ಎಷ್ಟು ಬೇಕೋ ಅಷ್ಟು ಮಾತ್ರ ದತ್ತಾಂಶ ಪಡೆಯಬೇಕು. ಅನಗತ್ಯ ಮಾಹಿತಿ ಸಂಗ್ರಹಿಸುವಂತಿಲ್ಲ.
- ಭದ್ರತಾ ಕ್ರಮಗಳು: ದತ್ತಾಂಶ ಸೋರಿಕೆಯಾಗದಂತೆ ತಡೆಯಲು ಅತ್ಯಾಧುನಿಕ ಭದ್ರತಾ

ತಂತ್ರಜ್ಞಾನಗಳನ್ನು ಅಳವಡಿಸಿಕೊಳ್ಳಬೇಕು.

- ಬ್ರೀಚ್ ನೋಟಿಫಿಕೇಶನ್: ದತ್ತಾಂಶ ಸೋರಿಕೆಯಾದಲ್ಲಿ ತಕ್ಷಣವೇ ದತ್ತಾಂಶ ಸಂರಕ್ಷಣಾ ಮಂಡಳಿ ಮತ್ತು ಸಂಬಂಧಪಟ್ಟ ವ್ಯಕ್ತಿಗೆ ಮಾಹಿತಿ ನೀಡಬೇಕು.

ಶಿಕ್ಷೆ ಮತ್ತು ದಂಡದ ಪ್ರಮಾಣ:

ಹಳೆಯ ಐಟಿ ಕಾಯ್ದೆಯಲ್ಲಿ ದಂಡದ ಪ್ರಮಾಣ ಕಡಿಮೆಯಿತ್ತು. ಆದರೆ DPDP ಕಾಯ್ದೆಯು ಅತ್ಯಂತ ಕಠಿಣವಾಗಿದೆ:

- ನಿಯಮಗಳ ಉಲ್ಲಂಘನೆಗಾಗಿ ಸಂಸ್ಥೆಗಳಿಗೆ ₹50 ಕೋಟಿಯಿಂದ ₹250 ಕೋಟಿಯವರೆಗೆ ದಂಡ ವಿಧಿಸಬಹುದು.
- ದತ್ತಾಂಶ ಸಂರಕ್ಷಣಾ ಮಂಡಳಿಯು (Data Protection Board of India) ಈ ದಂಡದ ಪ್ರಮಾಣವನ್ನು ನಿರ್ಧರಿಸುವ ಅಧಿಕಾರ ಹೊಂದಿದೆ.

ವಿನಾಯಿತಿಗಳು:

ಸರ್ಕಾರವು ರಾಷ್ಟ್ರೀಯ ಭದ್ರತೆ, ಸಾರ್ವಜನಿಕ ಸುವ್ಯವಸ್ಥೆ ಮತ್ತು ಅಪರಾಧಗಳ ತನಿಖೆಯ ಸಂದರ್ಭದಲ್ಲಿ ಈ ಕಾಯ್ದೆಯಿಂದ ಕೆಲವು ವಿನಾಯಿತಿಗಳನ್ನು ಹೊಂದಿದೆ.

ಸಮಕಾಲೀನ ಸವಾಲುಗಳು:

ಪ್ರಸ್ತುತ ಡಿಜಿಟಲ್ ವ್ಯವಸ್ಥೆಯು ಎರಡು ದಶಕಗಳ ಹಿಂದೆ ಕಲ್ಪಿಸಿಕೊಳ್ಳಲು ಅಸಾಧ್ಯವಾಗಿದ್ದ ಬೆದರಿಕೆಗಳನ್ನು ಎದುರಿಸುತ್ತಿದೆ, ಅವುಗಳೆಂದರೆ:

1. ಕೃತಕ ಬುದ್ಧಿಮತ್ತೆ ಮತ್ತು ಡೀಪ್‌ಫೇಕ್‌ಗಳು

ಜನರೇಟಿವ್ AI ಗಳು ಉತ್ತಮ ಗುಣಮಟ್ಟದ ಡೀಪ್‌ಫೇಕ್‌ಗಳ ರಚನೆಯನ್ನು ಶಕ್ತಗೊಳಿಸಿವೆ, ಇದನ್ನು ಹಣಕಾಸಿನ ವಂಚನೆ ಮತ್ತು ಚಾರಿತ್ರ್ಯ ಹರಣಕ್ಕಾಗಿ ಬಳಸಲಾಗುತ್ತಿದೆ. ಐಟಿ ಕಾಯ್ದೆಯ ಸೆಕ್ಷನ್ 66D (ವ್ಯಕ್ತಿತ್ವದ ಮೂಲಕ ವಂಚನೆ) ಅನ್ವಯಿಸಲಾಗಿದ್ದರೂ, ನಿರ್ದಿಷ್ಟ "AI ಹೊಣೆಗಾರಿಕೆ" ಕಾನೂನುಗಳ ಕೊರತೆಯಿಂದಾಗಿ ಈ ಅಪರಾಧಗಳಲ್ಲಿ ಬಳಸುವ ಸಾಧನಗಳ ಅಭಿವರ್ಧಕರನ್ನು ವಿಚಾರಣೆಗೆ ಒಳಪಡಿಸುವುದು ಕಷ್ಟಕರವಾಗಿದೆ.

2. ನ್ಯಾಯವ್ಯಾಪ್ತಿಯ ಅಡೆತಡೆಗಳು

ಸೈಬರ್ ಅಪರಾಧವು ಮೂಲಭೂತವಾಗಿ ಅಂತರರಾಷ್ಟ್ರೀಯ ಸ್ವರೂಪದ್ದಾಗಿದೆ. ಬೆಂಗಳೂರಿನ ನಾಗರಿಕನನ್ನು ವಂಚಿಸಲು ವಿದೇಶದಲ್ಲಿನ ಸರ್ವರ್ ಅನ್ನು ಬಳಸಿದರೆ, ಬಲವಾದ ಅಂತರರಾಷ್ಟ್ರೀಯ ಒಪ್ಪಂದಗಳು ಅಥವಾ ಪರಸ್ಪರ ಕಾನೂನು ಸಹಾಯ ಒಪ್ಪಂದಗಳಿಲ್ಲದೆ (MLATs) ಐಟಿ ಕಾಯ್ದೆಯ ಸೆಕ್ಷನ್ 75 ರಲ್ಲಿ ಉಲ್ಲೇಖಿಸಲಾದ "ಹೆಚ್ಚುವರಿ ಪ್ರಾದೇಶಿಕ" ಅನ್ವಯವನ್ನು ಜಾರಿಗೊಳಿಸುವುದು ಕಷ್ಟವಾಗುತ್ತದೆ.

3. ಮಧ್ಯವರ್ತಿ ಹೊಣೆಗಾರಿಕೆ

2021ರ ಮಧ್ಯವರ್ತಿ ಮಾರ್ಗಸೂಚಿಗಳು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ವೇದಿಕೆಗಳನ್ನು ಕುಂದುಕೊರತೆ ಅಧಿಕಾರಿಗಳನ್ನು ನೇಮಿಸಲು ಮತ್ತು ಕಾನೂನುಬಾಹಿರ ವಿಷಯವನ್ನು 36 ಗಂಟೆಗಳ ಒಳಗೆ ತೆಗೆದುಹಾಕಲು ಒತ್ತಾಯಿಸಿದವು. ಆದಾಗ್ಯೂ, ಸೆಕ್ಷನ್ 79 ರ ಅಡಿಯಲ್ಲಿ "ಸೇಫ್ ಹಾರ್ಬರ್" (Safe Harbor) ರಕ್ಷಣೆಯ ಬಗ್ಗೆ ಚರ್ಚೆ ಮುಂದುವರೆದಿದೆ, ಏಕೆಂದರೆ ವೇದಿಕೆಗಳು ಸೆನ್ಸಾರ್‌ಶಿಪ್ ಮತ್ತು ವೈರಲ್ ತಪ್ಪು ಮಾಹಿತಿಯ ತಡೆಗಟ್ಟುವಿಕೆಯ ನಡುವೆ

ಸಮತೋಲನ ಕಾಯ್ದುಕೊಳ್ಳಲು ಹೆಣಗಾಡುತ್ತಿವೆ.

4. ಡಾರ್ಕ್ ವೆಬ್:

ಡಾರ್ಕ್ ವೆಬ್ ಎನ್ನುವುದು ಅಂತರ್ಜಾಲದ ಅತ್ಯಂತ ನಿಗೂಢ ಮತ್ತು ಗುಪ್ತ ವಿಭಾಗವಾಗಿದ್ದು, ಇದನ್ನು ಗೂಗಲ್ ಅಥವಾ ಬಿಂಗ್‌ನಂತಹ ಸಾಮಾನ್ಯ ಸರ್ಚ್ ಇಂಜಿನ್‌ಗಳ ಮೂಲಕ ಪ್ರವೇಶಿಸಲು ಸಾಧ್ಯವಿಲ್ಲ. ಸೈಬರ್ ಕಾನೂನು ಮತ್ತು ಭದ್ರತೆಯ ದೃಷ್ಟಿಯಿಂದ ಡಾರ್ಕ್ ವೆಬ್ ಅತ್ಯಂತ ಸವಾಲಿನ ಕ್ಷೇತ್ರವಾಗಿದೆ ಏಕೆಂದರೆ ಇಲ್ಲಿ ನಡೆಯುವ ವ್ಯವಹಾರಗಳು ಹೆಚ್ಚಾಗಿ ಅಕ್ರಮ ಸ್ವರೂಪದ್ದಾಗಿರುತ್ತವೆ. ಮಾದಕ ದ್ರವ್ಯಗಳ ಮಾರಾಟ, ಕದ್ದ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಿವರಗಳು, ನಕಲಿ ದಾಖಲೆಗಳ ಸೃಷ್ಟಿ ಮತ್ತು ಹ್ಯಾಕಿಂಗ್ ಸೇವೆಗಳ ವ್ಯಾಪಾರವು ಅವ್ಯಾಹತವಾಗಿ ನಡೆಯುತ್ತದೆ. ಈ ವ್ಯವಹಾರಗಳಿಗೆ ಬಿಟ್‌ಕಾಯಿನ್ ಅಥವಾ ಮೊನೆರೊದಂತಹ ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿಗಳನ್ನು ಬಳಸುವುದರಿಂದ ಹಣದ ಮೂಲವನ್ನು ಪತ್ತೆಹಚ್ಚುವುದು ತನಿಖಾ ಸಂಸ್ಥೆಗಳಿಗೆ ಬಹುತೇಕ ಅಸಾಧ್ಯವಾಗುತ್ತದೆ. ಭಾರತೀಯ ಸೈಬರ್ ಕಾನೂನು ಚೌಕಟ್ಟಿನಲ್ಲಿ ಇಂತಹ ಚಟುವಟಿಕೆಗಳನ್ನು ಪತ್ತೆಹಚ್ಚಲು ವಿಶೇಷ ಸೈಬರ್ ಸೆಲ್‌ಗಳು ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತಿದ್ದರೂ, ಡಾರ್ಕ್ ವೆಬ್‌ನ ಗಡಿಯಿಲ್ಲದ ಸ್ವರೂಪ ಮತ್ತು ತಾಂತ್ರಿಕ ಸಂಕೀರ್ಣತೆಗಳು ಕಾನೂನು ಜಾರಿಗೊಳಿಸುವಲ್ಲಿ ಅಡೆತಡೆಗಳನ್ನು ಉಂಟುಮಾಡುತ್ತಿವೆ.

5. ಮೆಟಾವರ್ಸ್:

ಮೆಟಾವರ್ಸ್ ಎಂಬುದು ಇಂಟರ್ನೆಟ್‌ನ ಮುಂದಿನ ಹಂತವಾಗಿದ್ದು, ಇದನ್ನು ವರ್ಚುವಲ್ ಮತ್ತು ಆಗ್ಮೆಂಟೆಡ್ ರಿಯಾಲಿಟಿ ತಂತ್ರಜ್ಞಾನಗಳ ಸಂಗಮವೆಂದು ಕರೆಯಬಹುದು. ಇದು ಬಳಕೆದಾರರಿಗೆ ತಮ್ಮ ಡಿಜಿಟಲ್ ಅವತಾರಗಳ ಮೂಲಕ ಭೌತಿಕವಾಗಿ ಉಪಸ್ಥಿತರಿಲ್ಲದಿದ್ದರೂ ಸಹಜವಾಗಿ ಸಂವಹನ ನಡೆಸಲು, ಕೆಲಸ ಮಾಡಲು ಮತ್ತು ವ್ಯಾಪಾರ ಮಾಡಲು ಅನುವು ಮಾಡಿಕೊಡುವ ಒಂದು ಇಮ್ಮರ್ಸಿವ್ ಡಿಜಿಟಲ್ ಜಗತ್ತಾಗಿದೆ. ಸೈಬರ್ ಕಾನೂನಿನ ದೃಷ್ಟಿಯಿಂದ, ಮೆಟಾವರ್ಸ್‌ನಲ್ಲಿ ನಡೆಯುವ ವರ್ಚುವಲ್ ಕಿರುಕುಳ, ಆಸ್ತಿ ವಂಚನೆ ಮತ್ತು ದತ್ತಾಂಶ ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಳನ್ನು ನಿಯಂತ್ರಿಸುವುದು ದೊಡ್ಡ ಸವಾಲಾಗಿದೆ. ಇಲ್ಲಿನ ಗಡಿಯಿಲ್ಲದ ವ್ಯವಸ್ಥೆಯು ನ್ಯಾಯವ್ಯಾಪ್ತಿಯ ಸಮಸ್ಯೆಗಳನ್ನು ಸೃಷ್ಟಿಸುವುದರಿಂದ, ಭವಿಷ್ಯದಲ್ಲಿ ನಿರ್ದಿಷ್ಟ ಕಾನೂನು ತಿದ್ದುಪಡಿಗಳ ಅಗತ್ಯವಿದೆ.

6. ಬ್ಲಾಕ್‌ಚೈನ್ ತಂತ್ರಜ್ಞಾನ ಮತ್ತು ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿಗಳ ಕಾನೂನು ಸವಾಲುಗಳು

ಬ್ಲಾಕ್‌ಚೈನ್ ತಂತ್ರಜ್ಞಾನವು ಇಂದಿನ ಡಿಜಿಟಲ್ ಯುಗದಲ್ಲಿ ವಿಕೇಂದ್ರೀಕೃತ ಮತ್ತು ಪಾರದರ್ಶಕ ವ್ಯವಹಾರಗಳಿಗೆ ಹೊಸ ದಾರಿಯನ್ನು ತೆರೆದಿದ್ದರೂ, ಸೈಬರ್ ಕಾನೂನು ಜಾರಿಗೆ ಇದು ದೊಡ್ಡ ಸವಾಲಾಗಿದೆ. ಬ್ಲಾಕ್‌ಚೈನ್‌ನ ಮೂಲ ಸ್ವರೂಪವೇ 'ಬದಲಾಯಿಸಲಾಗದ' (Immutable) ಮತ್ತು 'ಅನಾಮಧೇಯ' (Anonymous) ಆಗಿರುವುದರಿಂದ, ಒಮ್ಮೆ ನಡೆದ ವ್ಯವಹಾರವನ್ನು ರದ್ದುಗೊಳಿಸಲು ಅಥವಾ ಅದನ್ನು ನಡೆಸಿದ ವ್ಯಕ್ತಿಯನ್ನು ಪತ್ತೆಹಚ್ಚಲು ಸಾಮಾನ್ಯ ತನಿಖಾ ಸಂಸ್ಥೆಗಳಿಗೆ ಅಸಾಧ್ಯವಾಗುತ್ತದೆ. ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿಗಳಾದ ಬಿಟ್‌ಕಾಯಿನ್ ಮತ್ತು ಎಥೆರಿಯಮ್‌ಗಳನ್ನು ಬಳಸಿ ನಡೆಯುವ ಹಣಕಾಸಿನ ವಹಿವಾಟುಗಳು ಯಾವುದೇ ಕೇಂದ್ರೀಯ ಬ್ಯಾಂಕ್‌ಗಳ ನಿಯಂತ್ರಣದಲ್ಲಿ ಇಲ್ಲದಿರುವುದು ಸೈಬರ್ ಅಪರಾಧಿಗಳಿಗೆ ವರದಾನವಾಗಿದೆ. ಅಪರಾಧಿಗಳು ಡಾರ್ಕ್ ವೆಬ್‌ನಲ್ಲಿ ಅಕ್ರಮ ವ್ಯವಹಾರಗಳನ್ನು ನಡೆಸಿ, ಹಣವನ್ನು ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿಗಳ ಮೂಲಕ ವರ್ಗಾವಣೆ ಮಾಡುವುದರಿಂದ ಹಣದ ಹರಿವನ್ನು (Money Trail) ಪತ್ತೆಹಚ್ಚುವುದು ಸೈಬರ್ ತನಿಖಾಧಿಕಾರಿಗಳಿಗೆ ಜಾಗತಿಕ ಮಟ್ಟದ

ಸಮಸ್ಯೆಯಾಗಿ ಪರಿಣಮಿಸಿದೆ.

ಭಾರತದಲ್ಲಿ ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿಗಳ ಕಾನೂನುಬದ್ಧತೆಯ ಬಗ್ಗೆ ಸುದೀರ್ಘ ಚರ್ಚೆಗಳು ನಡೆಯುತ್ತಿದ್ದು, ಪ್ರಸ್ತುತ ಇವುಗಳನ್ನು 'ವರ್ಚುವಲ್ ಡಿಜಿಟಲ್ ಆಸೆಟ್ಸ್' (VDA) ಎಂದು ಪರಿಗಣಿಸಿ ತೆರಿಗೆ ವ್ಯಾಪ್ತಿಗೆ ತರಲಾಗಿದೆ. ಆದರೂ, ಬ್ಲಾಕ್‌ಚೈನ್ ಆಧಾರಿತ ವಂಚನೆಗಳು, ಅಂದರೆ 'ರಗ್ ಪುಲ್' (Rug Pull) ವಂಚನೆಗಳು ಅಥವಾ ನಕಲಿ ಕ್ರಿಪ್ಟೋ ಹೂಡಿಕೆ ಯೋಜನೆಗಳನ್ನು ನಿಯಂತ್ರಿಸಲು ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯ್ದೆಯಲ್ಲಿ ನಿರ್ದಿಷ್ಟ ನಿಬಂಧನೆಗಳ ಕೊರತೆಯಿದೆ.

ಇದಲ್ಲದೆ, ಬ್ಲಾಕ್‌ಚೈನ್‌ನಲ್ಲಿ ಮಾಹಿತಿ ಸಂಗ್ರಹವಾದಾಗ ಅದನ್ನು ಅಳಿಸಿಹಾಕುವುದು ಅಸಾಧ್ಯವಾಗಿರುವುದರಿಂದ, ಇದು ಡಿಜಿಟಲ್ ವೈಯಕ್ತಿಕ ದತ್ತಾಂಶ ಸಂರಕ್ಷಣಾ (DPDP) ಕಾಯ್ದೆಯಡಿ ಇರುವ ವ್ಯಕ್ತಿಯ 'ದತ್ತಾಂಶ ಅಳಿಸುವಿಕೆಯ ಹಕ್ಕಿಗೆ' (Right to Erasure) ವ್ಯತಿರಿಕ್ತವಾಗಿದೆ. ಆದ್ದರಿಂದ, ಬ್ಲಾಕ್‌ಚೈನ್ ತಂತ್ರಜ್ಞಾನದ ಲಾಭಗಳನ್ನು ಪಡೆದುಕೊಳ್ಳುತ್ತಲೇ ಅದರ ಮೂಲಕ ನಡೆಯುವ ಆರ್ಥಿಕ ಅಪರಾಧಗಳನ್ನು ತಡೆಯಲು ಭಾರತಕ್ಕೆ ಒಂದು ಸಮಗ್ರವಾದ 'ಡಿಜಿಟಲ್ ಆಸ್ತಿ ನಿಯಂತ್ರಣ ಕಾಯ್ದೆ'ಯ ಅಗತ್ಯವಿದೆ.

ಶಿಫಾರಸುಗಳು:

ಇವತ್ತಿನ ಡಿಜಿಟಲ್ ಯುಗದಲ್ಲಿ ತಂತ್ರಜ್ಞಾನದಿಂದ ಅನೇಕ ಉಪಯೋಗಗಳಿದ್ದರೂ, ಈ ತಂತ್ರಜ್ಞಾನದ ಕ್ರಾಂತಿಯಿಂದ ಅನೇಕ ಹೊಸ ಸಮಸ್ಯೆಗಳನ್ನು ಕೂಡ ಎದುರಿಸುತ್ತಿದ್ದೇವೆ. ಅಂತಹ ಸಮಸ್ಯೆಗಳನ್ನು ಪರಿಹರಿಸಲು ಕೆಲವು ಶಿಫಾರಸುಗಳನ್ನು ಈ ಕೆಳಕಂಡಂತೆ ಸೂಚಿಸಲಾಗಿದೆ.

- ಏಕೀಕೃತ ಸೈಬರ್ ಭದ್ರತಾ ಕಾಯ್ದೆ: ಭಾರತಕ್ಕೆ ನಿರ್ದಿಷ್ಟವಾಗಿ ನಿರ್ಣಾಯಕ ಮೂಲಸೌಕರ್ಯ ರಕ್ಷಣೆ ಮತ್ತು ಡಿಜಿಟಲ್ ಆಡಳಿತದ ಮೇಲೆ ಕೇಂದ್ರೀಕರಿಸುವ ಸ್ವತಂತ್ರ ಸೈಬರ್ ಭದ್ರತಾ ಕಾಯ್ದೆಯ ಅಗತ್ಯವಿದೆ.
- ವಿಶೇಷ ನ್ಯಾಯಾಲಯಗಳು: ಡಿಜಿಟಲ್ ಸಾಕ್ಷ್ಯದ ತಾಂತ್ರಿಕ ಸ್ವರೂಪಕ್ಕೆ ಡಿಜಿಟಲ್ ಫೋರೆನ್ಸಿಕ್ಸ್‌ನಲ್ಲಿ ತರಬೇತಿ ಪಡೆದ ನ್ಯಾಯಾಧೀಶರು ಮತ್ತು ಪ್ರಾಸಿಕ್ಯೂಟರ್‌ಗಳನ್ನು ಹೊಂದಿರುವ ವಿಶೇಷ "ಸೈಬರ್ ನ್ಯಾಯಾಲಯಗಳ" ಅಗತ್ಯವಿದೆ.
- ಅಂತರರಾಷ್ಟ್ರೀಯ ಸಹಕಾರ: ಗಡಿಯಾಚೆಗಿನ ಸೈಬರ್ ಸಿಂಡಿಕೇಟ್‌ಗಳನ್ನು ಎದುರಿಸಲು ಬುಡಾಪೆಸ್ಟ್ ಕನ್ವೆನ್ಷನ್‌ನಂತಹ ಜಾಗತಿಕ ಒಪ್ಪಂದಗಳಲ್ಲಿ ಭಾಗವಹಿಸುವಿಕೆಯನ್ನು ಬಲಪಡಿಸುವುದು ಅತ್ಯಗತ್ಯ. ಅಂತಾರಾಷ್ಟ್ರೀಯ ಸೈಬರ್ ಅಪರಾಧಗಳನ್ನು ತಡೆಯಲು ವಿದೇಶಿ ತನಿಖಾ ಸಂಸ್ಥೆಗಳೊಂದಿಗೆ (Interpol ಇತ್ಯಾದಿ) ನೇರ ಸಂಪರ್ಕ ಸಾಧಿಸುವ ಪ್ರಕ್ರಿಯೆಯನ್ನು ಸರಳಗೊಳಿಸಬೇಕು.
- AI ನಿಯಂತ್ರಣ: AI ಅಭಿವೃದ್ಧಿಪಡಿಸುವ ಕಂಪನಿಗಳ ಮೇಲೆ ನೈತಿಕ ಹೊಣೆಗಾರಿಕೆಯನ್ನು (Ethical Accountability) ಹೇರುವ ಕಟ್ಟುನಿಟ್ಟಿನ ನಿಯಮಗಳನ್ನು ತರಬೇಕು.
- ಡಿಜಿಟಲ್ ಸಾಕ್ಷರತೆ: ಶಾಲಾ–ಕಾಲೇಜು ಹಂತದಲ್ಲೇ ಡಿಜಿಟಲ್ ಭದ್ರತೆಯ ಬಗ್ಗೆ ಪಠ್ಯಕ್ರಮ ಅಳವಡಿಸಬೇಕು.
- ಸಾರ್ವಜನಿಕ ಜಾಗೃತಿ: ಜನರಿಗೆ ಸೈಬರ್ ವಂಚನೆಗಳು, ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ರಕ್ಷಿಸಿಕೊಳ್ಳುವ ಬಗ್ಗೆ, ಡಿಜಿಟಲ್ ಭದ್ರತಾ ಕ್ರಮಗಳ ಬಗ್ಗೆ, ಅರಿವು ಮೂಡಿಸಬೇಕು.

ಕಾನೂನುಬದ್ಧ ಹಕ್ಕುಗಳ ಬಗ್ಗೆ ಮಾಹಿತಿ ನೀಡಬೇಕು. "ತಿದ್ದುಪಡಿ ಹಕ್ಕು" ಮತ್ತು "ಅಳಿಸಿಹಾಕುವ ಹಕ್ಕು" (Right to Erasure) ಬಗ್ಗೆ ಬೃಹತ್ ಸಾರ್ವಜನಿಕ ಜಾಗೃತಿ ಅಭಿಯಾನಗಳನ್ನು ನಡೆಸಬೇಕು.

ಉಪಸಂಹಾರ:

ಭಾರತದಲ್ಲಿ ತಂತ್ರಜ್ಞಾನವು ಕಾನೂನಿಗಿಂತ ವೇಗವಾಗಿ ಬೆಳೆಯುತ್ತಿದೆ. ಸೈಬರ್ ಅಪರಾಧಿಗಳು ಸುಧಾರಿತ AI ಪರಿಕರಗಳನ್ನು ಬಳಸುತ್ತಿರುವುದರಿಂದ, ನಮ್ಮ ತನಿಖಾ ಸಂಸ್ಥೆಗಳು ಮತ್ತು ಕಾನೂನು ಚೌಕಟ್ಟು ಪೂರ್ವಭಾವಿಯಾಗಿ ಕ್ರಿಯಾಶೀಲವಾಗಿರಬೇಕಾದ (Proactive) ಅನಿವಾರ್ಯತೆ ಇದೆ. ಭವಿಷ್ಯದಲ್ಲಿ, ಭಾರತವು "ಕೃತಕ ಬುದ್ಧಿಮತ್ತೆ ನಿಯಂತ್ರಣ ಕಾಯ್ದೆ" ಮತ್ತು ಗಡಿಯಾಚೆಗಿನ ಸೈಬರ್ ಅಪರಾಧಗಳನ್ನು ತಡೆಯಲು ಬಲವಾದ ಅಂತರರಾಷ್ಟ್ರೀಯ ಸಹಕಾರದ ಮೇಲೆ ಗಮನ ಹರಿಸಬೇಕಿದೆ.

ಒಟ್ಟಾರೆಯಾಗಿ ಹೇಳುವುದಾದರೆ, ಭಾರತದ ಸೈಬರ್ ಕಾನೂನು (Cyber Law) ಕೇವಲ ಶಾಸನಗಳ ಸಂಗ್ರಹವಲ್ಲ, ಅದು ಬದಲಾಗುತ್ತಿರುವ ಡಿಜಿಟಲ್ ಯುಗಕ್ಕೆ ಅನುಗುಣವಾಗಿ ವಿಕಸನಗೊಳ್ಳುತ್ತಿರುವ ಒಂದು ಜೈವಿಕ ಪ್ರಕ್ರಿಯೆ. ಐಟಿ ಕಾಯ್ದೆ 2000 ಒಂದು ಭದ್ರವಾದ ಅಡಿಪಾಯ ಹಾಕಿಕೊಟ್ಟರೆ, ಡಿಪಿಡಿಪಿ ಕಾಯ್ದೆ 2023 ನಾಗರಿಕರ ದತ್ತಾಂಶದ ಹಕ್ಕುಗಳನ್ನು ಬಲಪಡಿಸಿದೆ. ಆದರೆ, ಪ್ರಸ್ತುತ ತಾಂತ್ರಿಕ ಪ್ರಗತಿಯನ್ನು ಗಮನಿಸಿದರೆ, ಭಾರತಕ್ಕೆ ಒಂದು "ಸೈಬರ್ ಭದ್ರತಾ ಸಂಕಲ್ಪ" (Cyber Security Resolve) ಮತ್ತು ಶೀಘ್ರಗತಿಯ ತನಿಖಾ ವ್ಯವಸ್ಥೆಯ ಅಗತ್ಯವಿದೆ.

ಪರಾಮರ್ಶನ ಗ್ರಂಥಗಳು:

1. Duggal, P. (2024). Cyberlaw: The Indian Perspective. Universal Law Publishing.
2. Government of India. (2000). The Information Technology Act, 2000. Ministry of Electronics and Information Technology.
3. Government of India. (2023). The Digital Personal Data Protection Act, 2023. Gazette of India.
4. Gupta, A., & Sharma, R. (2025). AI and the Law: Navigating the Deepfake Crisis in India. Journal of Cyber Policy and Law, 12(2), 45–67.
5. Ministry of Electronics and Information Technology. (2021). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
6. Supreme Court of India. (2015). Shreya Singhal v. Union of India. AIR 2015 SC 1523.
7. Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) v. Union of India. (2017) 10 SCC 1.

Funding:

This study was not funded by any grant.

Conflict of interest:

The Authors have no conflict of interest to declare that they are relevant to the content of this article.