SIR மென்பொருளில் நடந்தது என்ன? தடயங்களை மறைக்கும் திட்டமிட்ட சதி!

ஒரு மாபெரும் திருட்டுத்தனத்தில் கையும் களவுமாக மாட்டிக்கொண்டால் திருடர்கள் செய்யும் முதல் வேலை, அதற்கான தடயங்களை மறைப்பது அல்லது அழிப்பதுதான். இந்தியத் தேர்தல் ஆணையம், 'வாக்காளர் பட்டியல் சிறப்பு தீவிர திருத்தம்' (SIR) என்ற பெயரில் திருடியிருப்பது பொன்னையோ பொருளையோ அல்ல; அதைவிடப் பல்லாயிரம் மடங்கு மதிப்பு வாய்ந்த ஜனநாயகத்தையும், மக்களின் மகத்தான வாக்கு உரிமையையும்தான்.

ஒரு கொலைக் குற்றத்தைவிடக் கொடிய குற்றத்தைச் செய்திருக்கிறது தேர்தல் ஆணையம். SIR பணிகளின் மூலம் வாக்குகள் எவ்வாறு திருடப்பட்டன என்பது குறித்த விவாதங்களும் போராட்டங்களும் தொடர்ந்து நடந்து வருகின்றன. ஆனால், ஒன்றிய அரசும் அதற்குத் துணைநிற்கும் தேர்தல் ஆணையமும் கல்நெஞ்சத்தோடு எதற்கும் அசைந்துகொடுக்காமல் இருக்கின்றன. ஒருபுறம் தேர்தல் ஆணையத்திற்கு எதிரான போராட்டங்கள் கடுமையாக ஒடுக்கப்படுகின்றன; இன்னொருபுறம் SIR செயல்பாடுகள் குறித்து தகவல் அறியும் உரிமைச் சட்டத்தின் (RTI) கீழ் எழுப்பப்படும் கேள்விகளுக்குத் தேர்தல் ஆணையம் பதிலளிக்க மறுத்து வருகிறது. தலைமைத் தேர்தல் ஆணையருக்கும் பிற தேர்தல் ஆணையர்களுக்கும் இடையே ஏற்பட்ட மோதல்கள் கூட, இந்தத் தொழில்நுட்ப ரீதியான மறைமுகச் சதிகள் தொடர்பானவைதான் என்பதை இங்கு நினைவுகூர வேண்டும்.

SIR சர்ச்சையின் மையப்புள்ளியாக இருக்கும் 'இசிஐநெட்' (ECINET) மென்பொருள் குறித்த தகவல்களைத் தேர்தல் ஆணையம் தொடர்ந்து மறைத்து வருகிறது. RTI மூலம் கேட்கப்பட்ட கேள்விகளுக்கு மழுப்பலான பதில்களே அளிக்கப்பட்டன. பலவீனமான காரணங்களைக் கூறி, மென்பொருளின் பெயரை வெளிப்படுத்தவோ, செயற்கை நுண்ணறிவு (AI) பயன்படுத்தப்படுகிறதா என்பதையும் அதற்கான பாதுகாப்பு நடவடிக்கைகள் என்ன என்பதையும் உறுதிப்படுத்தவோ தேர்தல் ஆணையம் மறுத்துவிட்டது. மோசடி எப்படி அரங்கேற்றப்பட்டது என்பதை நிரூபிக்க வேண்டுமானால், அதற்குப் பயன்படுத்தப்பட்ட கருவிகளை நாம் தெளிவாகப் புரிந்துகொள்ள வேண்டும்.

RTI கேள்விகளும் தேர்தல் ஆணையத்தின் மழுப்பல்களும்:

வாக்காளர் பட்டியலைச் சீரமைப்பதற்காக இந்தியத் தேர்தல் ஆணையம் மேற்கொண்ட 'வாக்காளர் பட்டியல் சிறப்பு தீவிர திருத்த' (SIR) பணியில் பயன்படுத்தப்பட்ட மென்பொருள் (Software) தொடர்பாக, தெலங்கானாவைச் சேர்ந்த சமூக ஆர்வலர் எம்.ஏ. முஜீப் அய்யூப் உள்ளிட்டோர் RTI சட்டத்தின்கீழ் எழுப்பிய கேள்விகளும், அதற்குத் தேர்தல் ஆணையம் அளித்த பதில்களும் பெரும் விவாதங்களை ஏற்படுத்தியுள்ளன.

வாக்காளர் பட்டியலில் உள்ள பிழைகள் மற்றும் முரண்பாடுகளைக் கண்டறியப் பயன்படுத்தப்பட்ட தொழில்நுட்பத்தின் வெளிப்படைத்தன்மையைக் கேள்விக்குள்ளாக்கும் வகையில் பின்வரும் முதன்மையான கேள்விகள் கேட்கப்பட்டன:

1. வாக்காளர் பட்டியலில் உள்ள முரண்பாடுகளைக் கண்டறியத் தேர்தல் ஆணையம் பயன்படுத்திய மென்பொருள், செயலி, அல்காரிதம் அல்லது செயற்கை நுண்ணறிவு (AI) தளத்தின் பெயர் மற்றும் அதன் பதிப்பு (Version) என்ன?
2. இந்த மென்பொருளானது வாக்காளர்களின் விவரங்களைத் தானியங்கி முறையில் (Automatically) 'சந்தேகத்திற்குரியவை' என வகைப்படுத்தி, சரிபார்ப்பு, திருத்தம் அல்லது நீக்கத்திற்குப் பரிந்துரைக்கிறதா?
3. இந்த SIR பணிகளின் ஏதேனும் ஒரு கட்டத்தில் செயற்கை நுண்ணறிவு (AI), இயந்திரக் கற்றல் (Machine Learning) அல்லது கணிப்பு பகுப்பாய்வு (Predictive Analytics) போன்ற தானியங்கி முடிவெடுக்கும் தொழில்நுட்பங்கள் பயன்படுத்தப்பட்டதா?
4. இந்த மென்பொருள் மூலம் தவறான அடையாளப்படுத்துதலால் தகுதியான உண்மையான வாக்காளர்களின் பெயர்கள் பட்டியலிலிருந்து நீக்கப்படாமல் இருக்க வழங்கப்பட்டுள்ள பாதுகாப்பு வழிமுறைகள் (Safeguards) என்ன?
5. இவ்வாறு மென்பொருளால் சுட்டிக்காட்டப்படும் முரண்பாடுகளை இறுதி நடவடிக்கை எடுப்பதற்கு முன்பாக ஆய்வு செய்யும் அதிகாரிகள் யார்? அதற்கான பணிப்பாய்வு (Workflow) என்ன?

இக்கேள்விகளுக்குத் தேர்தல் ஆணையம் நேர்மையான பதில்களை அளிக்காமல், திசைதிருப்பும் மழுப்பலான வாதங்களையே முன்வைத்துள்ளது.

பொய் 1: "வணிகப் பாதுகாப்பு மற்றும் அறிவுசார் சொத்துரிமை"

தேர்தல் ஆணையத்தின் வாதம்:

"மென்பொருளின் பெயர் மற்றும் அதன் பதிப்பு (Version) தொடர்பான விவரங்கள் வணிக ரகசியம், வர்த்தக ரகசியங்கள் மற்றும் அறிவுசார் சொத்துரிமை (Commercial confidence, trade secrets, and intellectual property) சார்ந்தவை என்பதால், RTI சட்டத்தின் பிரிவு 8(1)(d)ன் கீழ் இதற்கு விலக்கு அளிக்கப்பட்டுள்ளது."

இது உண்மையல்ல!

1. **பொது நலன் புறக்கணிக்கப்படுதல்:** ஒரு ஜனநாயக அமைப்பின் அடிப்படைத் தூண்கள் வெளிப்படைத்தன்மையும் (Transparency) பொறுப்புக்கூறலுமே (Accountability) ஆகும். தேர்தல் என்பது நாட்டின் ஜனநாயக அடித்தளம். அதில் பயன்படுத்தப்படும் அமைப்புகள் நம்பகமானவையா என்பதை அறிவது 140 கோடி மக்களின் அடிப்படை உரிமை. இரண்டு நிறுவனங்களின் "வணிக ரகசியத்தை" விட, "தேர்தல் அமைப்பின் மீதான மக்களின் நம்பிக்கை" என்பதே மிகப்பெரிய பொது நலன் சார்ந்த விஷயம். எனவே, பிரிவு 8(1)(d)ல் உள்ள பொது நலன் விதியைப் பயன்படுத்தி இத் தகவலை அளித்திருக்க வேண்டும்.
2. **தவறான பாதுகாப்பு அணுகுமுறை:** தொழில்நுட்ப உலகில், "ஒரு அமைப்பின் மென்பொருள் பெயரை ரகசியமாக வைப்பதன் மூலம் மட்டுமே அதனைப் பாதுகாப்பாக வைத்திருக்க முடியும்" என்ற அணுகுமுறை அறிவியல்பூர்வமாக நிராகரிக்கப்பட்ட ஒன்றாகும். உண்மையான பாதுகாப்பு என்பது மென்பொருளின் வலுவான கட்டமைப்பு (Robust Architecture) மற்றும் திறந்த மூலத் தணிக்கை (Open Source/Independent Audit) மூலம் மட்டுமே சாத்தியமாகும். மென்பொருள் பதிப்பு எண்ணை மறைப்பது சந்தேகங்களை அதிகரிக்குமே தவிர, பாதுகாப்புக்கு உத்தரவாதம் அளிக்காது.
3. பொதுத்துறை நிறுவனங்களுக்கு பொருந்தாத விதி: தனியார் நிறுவனங்களுக்கிடையேயான சந்தைப் போட்டியைக் கருத்தில் கொண்டு உருவாக்கப்பட்ட பிரிவு 8(1)(d)ஐ, தேர்தல் நடத்தும் ஒரு பொது அதிகார அமைப்பிற்குப் பயன்படுத்துவது சட்டத்தின் நோக்கத்தையே சிதைப்பதாகும்.
4. சர்வதேச நடைமுறைகள்: ஜெர்மனி, நெதர்லாந்து போன்ற நாடுகளில் மின்னணு வாக்குப்பதிவு இயந்திரங்களின் செயல்பாட்டில் "பொதுமக்களுக்கான வெளிப்படைத்தன்மை" (Public Verifiability) இல்லை என்பதற்காகவே அவை அரசியலமைப்புச் சட்டத்திற்கு எதிரானது என அறிவிக்கப்பட்டு ரத்து செய்யப்பட்டன. அயர்லாந்து போன்ற நாடுகளில் மென்பொருள் கட்டமைப்பு தொடர்பான விவரங்கள் பொதுமக்கள் தணிக்கைக்கு உட்படுத்தப்பட்ட பின்னரே பரிசீலிக்கப்பட்டன.

ஒரு ஜனநாயக அமைப்பில், வணிக நிறுவனங்களின் "வர்த்தக ரகசியத்தை" விட "வாக்காளர்களின் நம்பிக்கை" மிக உயர்ந்த இடத்தில் வைக்கப்பட வேண்டும். மென்பொருள்களின் முழு மூலக் குறியீட்டை (Source Code) வெளியிடாவிட்டாலும் கூட, அதன் மென்பொருள் பெயர் மற்றும் பதிப்பு போன்ற அடிப்படை விவரங்களை வெளிப்படுத்துவது வணிகப் போட்டியை எந்த வகையிலும் பாதிக்காது. மாறாக, அத்தகைய வெளிப்படைத்தன்மை மட்டுமே தேர்தல் ஆணையத்தின் மீதான மக்களின் நம்பகத்தன்மையை வலுப்படுத்தும். எனவே, இத்தகவலை மறுக்க பிரிவு 8(1)(d)ஐ பயன்படுத்துவது ஜனநாயக தத்துவத்திற்கு முற்றிலும் முரணானது.

பொய் 2: "புதிய மென்பொருள் எதுவும் பயன்படுத்தப்படவில்லை"

தேர்தல் ஆணையத்தின் வாதம்:

"SIR பணிக்காகப் புதிய மென்பொருள் எதுவும் உருவாக்கப்படவோ அல்லது வாங்கப்படவோ இல்லை; வாக்காளர்களைச் சேர்ப்பது அல்லது நீக்குவது குறித்து தொகுதி அளவிலான தேர்தல் பதிவு அதிகாரிகள்தான் (EROs) ஆதாரங்களின் அடிப்படையில் முடிவெடுக்கிறார்கள்."

இது மற்றொரு பொய் பிரச்சாரம்!

"புதிய மென்பொருள் இல்லை" என்று கூறினாலும், ஏற்கனவே உள்ள மென்பொருள்களிலேயே ஒரே மாதிரியான பெயர்கள் (Duplicates), முகவரி மாற்றங்கள் அல்லது போலி வாக்காளர்களைக் கண்டறியப் பின்னணியில் அல்காரிதம்கள் (Algorithms) செயல்படுகின்றன.

- மென்பொருள் அல்லது AI அளிக்கும் "நீக்கப்பட வேண்டியவர்களின் பட்டியல்" அல்லது "சந்தேகத்திற்குரியவர்கள் பட்டியல்" அடிப்படையிலேயே அந்தந்த கள அதிகாரிகளான வாக்குச்சாவடி நிலை அதிகாரிகள் (BLO) கள ஆய்விற்கே செல்கிறார்கள். இதனால், மென்பொருளின் வழிமுறைகளில் (Logic/Rules) சிறு தவறு இருந்தாலும், அது லட்சக்கணக்கான வாக்காளர்களைப் பாதிக்கும்.



மனுஷ்ய புத்திரன்
மாநில ஆலோசகர்
தி.மு.க. தகவல் தொழில்நுட்ப அணி

- களத்தில் உள்ள BLO அதிகாரிகளுக்குப் பணிச்சுமை அதிகமாக இருக்கும் சூழலில், மென்பொருள் கொடுக்கும் பரிந்துரைகளை அவர்கள் 100% நேரில் சென்று சரிபார்க்கிறார்களா என்பது கேள்விக்குறியே. பெரும்பாலான நேரங்களில், மென்பொருள் சுட்டிக்காட்டும் பெயர்களை அதிகாரிகள் விரிவான விசாரணையின்றி நீக்கிவிடும் ஆபத்து உள்ளது. இதன் காரணமாகவே, லட்சக்கணக்கான வாக்காளர்களின் பெயர்கள் அவர்களுக்குத் தெரியாமலேயே பட்டியலிலிருந்து நீக்கப்பட்ட சம்பவங்கள் (தெலங்கானா உள்ளிட்ட பிற மாநிலத் தேர்தல்களில்) நடந்துள்ளன.
- மென்பொருள் எவ்வாறு வாக்காளர்களைப் பிரித்தெடுக்கிறது (Inclusion/Exclusion criteria) என்பதற்கான "மூலக் குறியீடு" (Source Code) அல்லது "விதிகள்" (Rules) பொதுத் தணிக்கைக்கு உட்படுத்தப்படுவதில்லை. ஒரு குறிப்பிட்ட சமூகம், பகுதி அல்லது குறிப்பிட்ட வயதுடைய வாக்காளர்களின் பெயர்கள் அதிகளவில் விடுபடும்போது, அதற்கு மென்பொருளின் பிழையா அல்லது அதிகாரிகளின் பிழையா என்பதைக் கண்டறியச் சுயாதீனத் தணிக்கை (Independent Audit) வசதி இல்லை.
- வாக்காளர் பட்டியல் திருத்தம் (SIR) மற்றும் தேர்தல் மேலாண்மைப் பணிகளில் பயன்படுத்தப்படும் மென்பொருள்களை (எ.கா: ECINET போன்றவை) அரசியல் கட்சிகளின் தேர்தல் முகவர்கள் (Election Agents / Polling Agents) நேரடியாக அணுகவோ, தணிக்கை செய்யவோ முடியாத நிலை குறித்துத் தீவிரமான குற்றச்சாட்டுகள் முன்வைக்கப்படுகின்றன. தேர்தல் முகவர்களுக்கு வாக்காளர் பட்டியலின் இறுதிப் பிரதி (Hard Copy/PDF) மட்டுமே வழங்கப்படுகிறது. ஆனால், அந்தப் பட்டியலிலிருந்து பெயர்கள் எதன் அடிப்படையில் நீக்கப்பட்டன அல்லது சேர்க்கப்பட்டன என்ற மென்பொருளின் தரவுப் பின்னணி (Data Logs/System Audit Trails) முகவர்களின் பார்வைக்குக் கிடைப்பதில்லை. மென்பொருள் எந்தக் காரணியைக் (Logic / Rules) கொண்டு ஒரு வாக்காளரை "சந்தேகத்திற்குரியவர்" எனக் சுட்டப்படுகிறது (Flagging) என்பதைத் தேர்தல் முகவர்களோ அல்லது அரசியல் கட்சிகளோ சரிபார்க்க அனுமதி இல்லை. தவறான முடிவுகளை சரி செய்ய தேர்தல் அதிகாரிகள், முகவர்கள் அணுக முடியாதபடி மையப்படுத்தப்பட்ட கட்டுப்பாட்டு அமைப்பு உருவாக்கப்பட்டுள்ளது.

புதிய தொழில்நுட்ப மாற்றங்களை மறைத்தல்:

SIR போன்ற தீவிரத் திருத்தப் பணிகளின் போது, தரவுத்தளங்களை ஒருங்கிணைத்தல் (Database Integration), ஆதார் இணைப்பு சரிபார்ப்பு அல்லது தானியங்கி ஒப்பிடுதல் போன்ற புதிய அம்சங்கள் (Features) மென்பொருளில் சேர்க்கப்படுகின்றன. "புதிய மென்பொருள் வாங்கப்படவில்லை" என்று கூறுவது தொழில்நுட்ப ரீதியாகச் சரியாக இருக்கலாம்; ஆனால் பயன்பாட்டில் உள்ள மென்பொருளில் செய்யப்பட்ட மாற்றங்கள் மற்றும் புதுப்பிப்புகள் (Updates/Upgrades) என்ன? என்பதை வெளிப்படுத்தாமல் இருப்பது வெளிப்படைத் தன்மைக்கு முரணானது.

திரிணாமுல் காங்கிரஸ் (TMC) எம்.பி.க்களான சாகேத் கோகலே மற்றும் டெரெக் ஓ பிரையன் ஆகியோர், தேர்தல் ஆணையத்தின் இந்த ரகசியத்தன்மை பெரும் சந்தேகத்தை ஏற்படுத்துவதாகக் குற்றம் சாட்டியுள்ளனர். இது வெளிப்படையான தேர்தல் திருத்தம் அல்ல; மாறாக திட்டமிட்ட "மென்பொருள் மூலமான தேர்தல் முறை கேடு" (Software Intensive Rigging) என்று அவர்கள் விமர்சித்துள்ளனர். 'டி.சி.எஸ்.' (TCS) நிறுவனம் உருவாக்கிய 'இ.சி.ஐ.நெட்' (ECINET) மென்பொருளின் பங்களிப்பைத் தேர்தல் ஆணையம் ஏன் வெளிப்படையாக அறிவிக்கவில்லை என்றும் கேள்வி எழுப்பப்பட்டுள்ளது.

டிஜிட்டல் உரிமைகள் அமைப்பான 'இன்டர்நெட் ஃப்ரீடம் ஃபவுண்டேஷன்' (IFF) மற்றும் பல ஆர்வலர்கள், முறையான தணிக்கை அல்லது பொது விவரங்கள் இல்லாமல் இந்த அல்காரிதம்கள் செயல்படுவதாகக் குறிப்பிட்டுள்ளனர். இரண்டு தசாப்தங்கள் பழமையான தரவுகளுடன் ஒப்பிட்டு இந்த மென்பொருள் தானாகவே வாக்காளர்களை நீக்குவதால், நாடு முழுவதும் கோடிக் கணக்கான தகுதியான இந்தியக் குடிமக்களின் வாக்குரிமை பறிபோகும் ஆபத்து உள்ளதாக எச்சரித்துள்ளனர்.

செயற்கை நுண்ணறிவு (AI) மூலம் நடந்திருக்கக்கூடிய முறைகேடுகள்:

செயற்கை நுண்ணறிவு தொழில்நுட்பம் SIR முறைகேடுகளுக்குப் பெருமளவு பயன்படுத்தப்பட்டிருக்கிறது என்ற சந்தேகங்கள் வலுத்துள்ளன. இதுகுறித்த கேள்விகளுக்குத் தேர்தல் ஆணையம் பதிலளிக்க மறுக்கிறது.

1. தரவு அடிப்படையிலான அல்காரிதம் முறைகேடு:

செயற்கை நுண்ணறிவு மாதிரிகள் (AI Models) அவற்றுக்கு வழங்கப்படும் தரவுகளைக் கொண்டுதான் (Training Data) கற்றுக்கொள்கின்றன. வாக்காளர் பட்டியலில் உள்ள பெயர்கள், முகவரிகள், சமூகப் பின்னணி அல்லது குறிப்பிட்ட பகுதியின் மக்கள்தொகை விவரங்களை அடிப்படையாகக் கொண்டு, குறிப்பிட்ட சில பிரிவினரின் பெயர்களை மட்டும் "சந்தேகத்திற்குரியவை" (Demographic Duplicates/Deficiencies) என்று சுட்டிக்காட்டும் வகையில் அல்காரிதம்களை வடிவமைக்க முடியும்.

- முறைகேடு நடக்கும் விதம்: எதிர்க்கட்சிகளுக்கு ஆதரவான வாக்குவங்கிகள் அதிகம் உள்ள பகுதிகள் அல்லது குறிப்பிட்ட சமூகத்தினர் (சிறுபான்மையினர்/முஸ்லிம்கள்) வசிக்கும் பகுதிகளில் உள்ள வாக்காளர் விவரங்களை இந்த AI மென்பொருள் தீவிரமாக ஸ்கேன் செய்து, அவற்றில் உள்ள சிறு எழுத்துப் பிழைகள் (Spelling mistakes) அல்லது முகவரி முரண்பாடுகளைக் காரணம் காட்டி, அவற்றை 'நீக்கப்பட வேண்டியவை' என்ற பட்டியலில் தானாகவே வகைப்படுத்தலாம்.
- தெலங்கானா உதாரணம்: இந்தியாவில் 'வெப்லான்ச்' (Weblaunches) மற்றும் தெலங்கானாவில் பயன்படுத்தப்பட்ட AadhaarVoter ID linking (EHR) அல்காரிதம் மூலம் 2018ஆம் ஆண்டு முறையான களஆய்வின்றி லட்சக்கணக்கான வாக்காளர் பெயர்கள் நீக்கப்பட்டதாகப் புகார்கள் எழுந்தன. அல்காரிதம் செய்த தவறுகளால் உண்மையான வாக்காளர்கள் கடுமையாகப் பாதிக்கப்பட்டனர்.

2. தானியங்கி தரவுப் பொருத்தம் மற்றும் தவறான நீக்கம்: (Automated Data Matching & False Positives)

இயந்திரக் கற்றல் (Machine Learning) அல்காரிதம்கள் இரு வேறு தரவுத்தளங்களை (Database) ஒப்பிடும்போது 'ஒரே மாதிரியான பெயர்கள்' (Soundex or Fuzzy Matching அல்காரிதம்) இருந்தால், அவர்களை ஒரே நபர் என்று தவறாகக் கணிக்க வாய்ப்புள்ளது.

- **முறைகேடு நடக்கும் விதம்:** உதாரணமாக, ஒரு தொகுதியில் " அப்துல் ரஹீம், தந்தை பெயர்: ஷேக் அப்துல்லா " என்ற பெயரில் இருவேறு வார்டுகளில் இருவர் இருந்தால், AI தொழில்நுட்பம் அவர்களின் புகைப்படம் அல்லது முகவரியை அரைகுறையாகப் பொருத்திப் பார்த்து, இருவரும் ஒருவரே என்று முடிவு செய்து ஒரு பெயரைத் தானாகவே நீக்கப் பரிந்துரைக்கலாம் (False Positive).
- **அமெரிக்க உதாரணம்:** அமெரிக்காவில் 'Interstate Crosscheck' என்ற அல்காரிதம் பயன்படுத்தப்பட்டபோது, அது வெவ்வேறு நபர்களை ஒரே நபர் என்று தவறாக அடையாளம் கண்டு லட்சக் கணக்கான சிறுபான்மையின வாக்காளர்களைப் பட்டியலிலிருந்து நீக்கியது தொழில்நுட்ப ரீதியாக நிரூபிக்கப்பட்டது.

3. இலக்கு வைக்கப்பட்ட வாக்காளர் ஒடுக்கம்: (Targeted Voter Suppression via Geofencing)

புவியியல் தகவல் அமைப்பு (GIS) மற்றும் இயந்திரக் கற்றல் மூலம் ஒரு குறிப்பிட்ட தேர்தல் தொகுதியின் வாக்குப்பதிவு வரலாற்றை (Voting history) பகுப்பாய்வு செய்ய முடியும்.

- **முறைகேடு நடக்கும் விதம்:** எந்தெந்த வாக்குச்சாவடிகளில் (Booths) ஆளுங்கட்சிக்கு ஆதரவு குறைவாக இருக்கிறது என்பதை AI மூலம் கண்டறிந்து, அந்தக் குறிப்பிட்ட புவியியல் எல்லைக்குள் (Geofencing) உள்ள வாக்காளர்களின் தரவுகளில் மட்டும் மென்பொருள் மூலமாகத் திருத்தங்கள் அல்லது இட மாற்றங்களைச் செய்து குழப்பத்தை ஏற்படுத்தலாம். இதன் மூலம் தேர்தல் நாளன்று அவர்கள் வாக்குச்சாவடிக்கு வரும்போதுதான் பெயர் விடுபட்டிருப்பது தெரியவரும்.

4. கறுப்புப்பெட்டி தொழில்நுட்பம் மற்றும் மனித தணிக்கையின்மை: (Black Box AI & Lack of Oversight)

'பிளாக் பாக்ஸ்' (Black Box) என்பது ஒரு AI அல்காரிதம் எவ்வாறு ஒரு முடிவை எடுத்தது என்ற காரணத்தை மனிதர்களால் எளிதில் கண்டறிய முடியாத ஒரு தொழில்நுட்பச் சூழலாகும்.

- **முறைகேடு நடக்கும் விதம்:** மென்பொருள் ஒரு வாக்காளரை "முறையற்றவர்" என்று பட்டியலிட்டதும், அதைச் சரிபார்க்கும் வாக்குச்சாவடி நிலை அதிகாரிகள் (BLOs), மென்பொருளின் முடிவை இறுதி உண்மை என்று நம்பி (Automation Bias), கள ஆய்வு செய்யாமலேயே பெயர்களை நீக்கிவிடுவார்கள். RTIயில் இதற்கான பாதுகாப்பு வழிமுறைகள் என்ன என்ற கேள்விக்குத் தேர்தல் ஆணையம் உரிய பதில் அளிக்காதது இந்தச் சந்தேகத்தை வலுப்படுத்துகிறது.
- **பொதுத் தணிக்கையின்மை:** இந்தியாவின் இன்டர்நெட் ஃப்ரீடம் ஃபவுண்டேஷன் (IFF) போன்ற அமைப்புகள், தேர்தல் ஆணையம் பயன்படுத்தும் அல்காரிதம்கள் பொது தணிக்கைக்கு (Public Audit) உட்படுத்தப்படாதவரை, டிஜிட்டல் முறையில் வாக்காளர்களைப் பட்டியலிலிருந்து விலக்குவது மிக எளிதாக நடக்கும் என்று தொடர்ந்து எச்சரித்து வருகின்றன.

இதுதான் SIRஇல் நடந்த மோசடிகளில் தொழில்நுட்பம் பயன்படுத்தப்பட்ட விதம்.

கடந்த காலங்களில் மின்னணு வாக்குப் பதிவு இயந்திரங்கள் தொடர்பான குற்றச்சாட்டுகளில் சந்தேகம் எழுப்பியவர்களையே தண்டித்து அச்சுறுத்தும் நடவடிக்கைகள் மேற்கொள்ளப்பட்டன.

நீதிமன்றங்கள் தேர்தல் ஆணையத்தின் தில்லுமுல்லுகளுக்கு எதிரான வழக்குகளில் ஆணையத்தின் தன்னாட்சித் தன்மைக்கு அதீத முக்கியத்துவம் அளித்துக் கையாண்ட மென்மையான போக்கு மற்றும் தேர்தல் ஆணையரை அவரது குற்றங்களிலிருந்து பாதுகாக்கும் சட்டத்திருத்தம் ஆகியவை காரணமாகவே, எந்தக் குற்றத்தையும் தைரியமாகச் செய்யலாம் என்ற துணிச்சலைத் தேர்தல் ஆணையம் பெற்றுள்ளது.