பாடப்பிரிவு 11 இணையதளச் சட்டம்

பாடத் திட்ட அமைப்பு

11.0 பாட முன்னுரை

உலகெங்கிலும் தகவல் தொடர்பு தொழில்நுட்பங்கள் நெட்வொர்க்குகள், சாதனங்கள் மற்றும் சேவைகளின் விரைவான பயன்பாட்டின் சகாப்தத்தில், இணையவெளி ஒரு புதிய தகவல்தொடர்பு ஊடகமாக உருவெடுத்துள்ளது. சர்வதேச தொலைத்தொடர்பு ஒன்றியத்தின் (ஐ.டி.யு) கூற்றுப்படி, சர்வதேச இணைய அலைவரிசை உலகம் முழுவதும் வேகமாக வளர்ந்து வருகிறது, மேலும் இந்தியா உலகின் முன்னணி நாடுகளில் ஒன்றாகும். இந்தியாவில் நகரங்கள் மற்றும் கிராமங்களில் இணையம் வேகமாக வளர்ந்து வருகிறது. அதிகமான மக்கள் மொபைல் தொலைபேசிகளைப் பயன்படுத்துகின்றனர், இது நாட்டில்

அதன் வளர்ச்சியை மேலும் துரிதப்படுத்தியுள்ளது. புதிய மெய்நிகர் வெளி இவ்வாறு பல சமூக மற்றும் தேசிய பிரச்சினைகளுக்கு வழிவகுத்துள்ளது மற்றும் தொழில்நுட்பத்தால் இயக்கப்படும் இணையதளக் குற்றங்களை சமாளிக்கவும், தனி நபரின் உரிமை மற்றும் அறிவுசார் உரிமைகள் பாதுகாக்கவும் புதிய சவால்களை முன்வைத்துள்ளது.

இணையதள, இணையவெளி குற்றங்கள் மற்றும் அதிலிருந்து வெளிவரும் பிற சிக்கல்கள் பற்றிய கண்ணோட்டத்தை இந்த பாடப்பிரிவு உங்களுக்கு வழங்குகிறது.

11.1 படிப்பு நோக்கம்

இந்த பாடப்பிரிவைப் படித்த பிறகு, நீங்கள் பின்வருவனவற்றைச் செய்ய முடியும்:

- இணையவெளி பற்றி கருத்து விவாதிக்க;
- இணையவெளி ஒழுங்குமுறையின் தேவையை விளக்கவும்;
- இணையவெளி காரணமாக எழுந்த பல்வேறு சிக்கல்களை கோடிட்டுக் காட்டவும்;
- தகவல் தொழில்நுட்ப (ஐ.டி) சட்டத்தின் கீழ் இணையதளக் குற்றங்கள் மற்றும் குற்றங்களை விவரிக்கவும்;
- இந்தியாவில் இணையவெளியை ஒழுங்குபடுத்தும் சட்டத்தைப் பற்றி அறிந்து கொள்ளவும் முடியும்.

11.2 இணையவெளியின் விளக்கம்

இணையவெளி என்பது பல்வேறு கணினி அமைப்புகள் மற்றும் மொபைல் போன்களை இணைக்கும் இணையத்தின் உதவியுடன் பல்வேறு நிகழ்வுகள், கருத்துக்களைப் பகிர்தல் ஆகியவை நடைபெறும் ஒரு இடத்தைக் குறிக்கிறது.

மின்னணு தகவல்தொடர்பின் வருகை மற்றும் வளர்ச்சியுடன், "இணையவெளி" என்ற வார்த்தை நமது அன்றாட மொழியில் நுழைந்துள்ளது. ஆனால் இந்த வார்த்தை எதைக் குறிக்கிறது? ஒரு சாதாரண நபருக்கு, இணையவெளி என்பது வரம்புகளைக் கொண்டிராத ஒரு விர்ச்சுவல் பகுதியைக் குறிக்கிறது, அங்கு ஒருவர் மக்களைச் சந்திக்கவும், இணையம் மூலம் எந்தவொரு விஷயத்தைப் பற்றிய தகவலையும் கண்டறியவும் முடியும். இணையவெளியில் நீங்கள்

கிட்டத்தட்ட எந்த கேள்விக்கும் சரியான, தவறான அல்லது குழப்பமான பதிலைக் காணலாம். இணையவெளி பற்றிய இந்த விளக்கம் 100% துல்லியமானது அல்ல, ஆனால் அதன் முக்கியமான பண்புகளில் சிலவற்றை அதன் சமூக பரிமாணம் மற்றும் அதன் செயல்பாடு பற்றி சுட்டிக்காட்டுகிறது.

ரெபேக்கா பிரையண்டின் கூற்றுப்படி, இணையவெளி என்பது, "தகவல்தொடர்பு, மின்னணு தகவல்தொடர்பு ஆகியவற்றின் புதிய ஊடகத்தை பிரதிபலிக்கிறது, இது வேகமாக காலாவதியாகிறது, அல்லது பாரம்பரிய தகவல்தொடர்பு முறைகளை மாற்றுகிறது. எனவே, விண்வெளி மற்றும் இணையவெளி ஆகியவை தோராயமாக சமமான கருத்தியல் உறுப்புகளாக கணக்கிடப்படலாம் என்று தோன்றுகிறது, குறைந்தபட்சம் இடத்தின் தூரம், அளவு, நேரம் மற்றும் பாதை ஆகிய நான்கு பொதுவான துணை கருத்துகளைப் பகிர்ந்து கொள்ளும் அர்த்தத்தில் உள்ளது.

வேறுபாடுகள் இருந்தபோதிலும், இணையவெளி என்பது ஒரு வழியில், உலகத்துடன் நெருக்கமாக இணைக்கப்பட்டுள்ளது. இணையவெளி அதன் இருப்பிற்காக, வன்பொருள் மற்றும் மென்பொருள், கேபிள்கள் மற்றும் ரூட்டர்களை சார்ந்துள்ளது - இது ஒரு இடத்தில் இருக்கும் பொருட்களின் இடையே உள்ள இடைவெளியைப் பொறுத்தது. மேலும், நிச்சயமாக, இரண்டுக்கும் இடையிலான இந்த நெருக்கமான இணைப்பு, இடைவெளி இருந்தால், எதையும் சார்ந்தது அல்ல என்ற ஒரு அடிப்படை வேறுபாட்டையும் பிரதிபலிக்கிறது".

11.2.1 இணையவெளியின் சிறப்பியல்புகள்

டேவிட் பி.விட்டில், "சைபர்ஸ்பேஸ்: தி ஹ்யூமன் டைமன்ஷன்" என்ற புத்தகத்தில், சைபர்ஸ்பேஸின் மூன்று பண்புகளை அடையாளம் கண்டுள்ளார்: (1) இது ஒரு பௌதிக இருப்பிடம் அல்ல மாறாக ஒரு விர்ச்சுவல் இடம். (2) சைபர் ஸ்பேஸில் நுழைவதற்கு அணுகல் சாதனம் தேவை. அதாவது டிஜிட்டல் கம்ப்யூட்டிங் சக்தி மற்றும்/அல்லது மென்பொருள் போன்ற செயற்கையான செயலாக்க பொறிமுறையுடன் ஒருவருக்கு ஒருவித திடமான அணுகல் சாதனம் (கணினித் திரை, தொலைபேசி, முனையம் போன்றவையாக இருக்கலாம்) தேவை. மேலும் அது உறுதியான இணைப்புகளின் நெட்வொர்க்கில் உள்ள பிற அணுகல் சாதனங்களுடன் இணைக்கப்பட வேண்டும்.(3) இது தனிநபர்கள் மற்றும் தனிநபர்களின் குழுக்களுக்கு இடையேயான தொடர்பு மற்றும்

தகவல்தொடர்பு மற்றும் அவர்களின் படைப்பு வெளியீடு ஆகியவற்றை செயல்படுத்துகிறது.

11.2.2 இணையவெளியிலிருந்து எழும் சிக்கல்கள் மற்றும் ஒழுங்குமுறைக்கான தேவை

இன்று புதிய தகவல்தொடர்பு தொழில்நுட்பங்கள், மொபைல் போன்கள் மற்றும் பிற தகவல்தொடர்பு சாதனங்களின் பயன்பாடு ஆகியவை உலகளாவிய அளவில் அதிகார வரம்பு பற்றிய பாரம்பரிய கருத்துக்கு சவால் விடுகின்றன. இது ஒரு தனிநபரின் தனியுரிமையை ஆக்கிரமிப்பதற்கான சாத்தியத்திற்கு வழிவகுத்துள்ளது. இணையவழி சமூக ஊடக குற்றங்கள், வதந்தி பரப்புதல், மின்னஞ்சல் ஸ்பூ஼பிங், ஸ்பேம்கள், இணைய பின்தொடர்தல், அவதூறு மற்றும் பல்வேறு இணையவழி கிரைம்களின் பிரச்சினைகளை சமாளிக்க பயனுள்ள சட்டம் இருக்க வேண்டும். ஏனெனில் இந்த குற்றங்களின் தாக்கம் வழக்கமான குற்றங்களை விட அதிகமாக இருக்கலாம். இந்த இணையவழி குற்றங்கள் பொதுவாக பின்வருவனவற்றால் செய்யப்படுகின்றன - போலி அடையாளத்தைப் பயன்படுத்தும் நபர், உடனடியாகவும் எளிதாகவும் அடையாளம் காண முடியாதவர் எனலாம்.

மேலும், பெயர் தெரியாததாலும், புழக்கத்தின் எளிமையாலும், இது பலருக்கு சமூக விவாதங்களை வழிவகுத்தது. பேச்சுரிமை, கருத்துச் சுதந்திரம் போன்ற இரு கருத்துக்களின் அடிப்படையில் நல்லிணக்கத்தைக் கோரும் பல சமூக விவாதங்களுக்கு இது வழிவகுத்துள்ளது. இது தவிர, கடுமையான ஒழுங்குமுறைக்கு அழைப்பு விடுக்கும் முக்கிய பகுதிகள்; அறிவுசார் சொத்து மேலாண்மை மற்றும் டிஜிட்டல் ஊடகங்களில் மீறல்களைத் தடுப்பது; பயங்கரவாதம் பரவுதல், எல்லை தாண்டிய வரிவிதிப்பு; வணிக நிறுவனங்கள் வணிக வாய்ப்புகளை இழக்க வழிவகுக்கும் தரவு மீறல்களால் பாதிக்கப்படக்கூடியவை என்பதால், இணைய பாதுகாப்பு ஒரு மதிப்புமிக்க விவகாரமாகும். எனவே அங்கீகரிக்கப்படாத அணுகல், தரவு / தகவலை மாற்றுதல் அல்லது அகற்றுதல், தரவு திருட்டு ஆகியவற்றிலிருந்து பாதுகாக்க வேண்டும்; தொழில்துறைகள், தனிநபர்கள் மற்றும் அரசாங்க நிறுவனங்களின் அங்கீகாரம், தரவு பாதுகாப்பு மற்றும் தரவு தனியுரிமை; குறியாக்கம்; பொருட்கள் மற்றும் சேவைகளின் தவறாக வழிநடத்தும் விளம்பரங்களிலிருந்து மின்-நுகர்வோரைப் பாதுகாத்தல், அவர்களுக்குத் தகவலறிந்த மற்றும் அர்த்தமுள்ள தெரிவுகளைச் செய்வதற்கு உதவுகிறது.

தனிநபர்களின் தனியுரிமையை மதித்து வணிக நிறுவனங்கள் நுகர்வோர் தகவல்களை பொறுப்புடன் நிர்வகிக்க வேண்டும், ஆனால் இதற்கு தரவு பரிமாற்றம் மற்றும் பயன்பாட்டை கட்டுப்படுத்தும் கடுமையான கட்டுப்பாட்டாளர்கள் தேவை.

தன் மதிப்பீடு 1

குறிப்பு: உங்கள் பதில்களுக்கு கீழே உள்ள இடத்தைப் பயன்படுத்தவும்

உங்கள் பதில்களை இந்த பாடப் பகுதியின் இறுதியில் கொடுக்கப்பட்ட பதில்களுடன் சரிபார்த்துக் கொள்ளவும்.

1) இணையவெளியின் பண்புகள் யாவை ?

.....

.....

.....

.....

.....

.....

2) நமக்கு ஏன் இணையவெளி ஒழுங்குமுறை தேவை?

.....

.....

.....

.....

.....

11.3 சர்வதேச மற்றும் தேசிய இணையவெளி சட்டங்கள்

இந்த பிரிவில் இணையவழியை நிர்வகிக்கும் சர்வதேச மற்றும் தேசிய சட்டங்களைப் பற்றி சுருக்கமாக விவாதிப்போம்.

11.3.1 சர்வதேச சட்டம்

UNCITRAL மாதிரி சட்டம் 1996, இ-கையொப்பம் மீதான மாதிரி சட்டம், 2001 மற்றும் சர்வதேச மின்னணு

தகவல்தொடர்புகளின் பயன்பாடு குறித்த ஐக்கிய நாடுகள் உடன்படிக்கை ஒப்பந்தங்கள், 2005 இணையவெளி தொடர்பான சில சர்வதேச முன்முயற்சிகளை உருவாக்குகின்றன.

UNCITRAL மாதிரி சட்டம் 1996 - E-Commerce பற்றிய முதல் மாதிரி சட்டம் 1996 ஆம் ஆண்டில் சர்வதேச வர்த்தகம் மற்றும் சட்டம் மீதான ஐக்கிய நாடுகள் ஆணையத்தால் (UNCITRAL) ஏற்றுக்கொள்ளப்பட்டது. ஐக்கிய நாடுகள் சபையின் பொதுச் சபை 1997 சனவரி 30ஆம் தேதி ஒரு தீர்மானத்தை நிறைவேற்றியது. இச்சட்டத்தின் முக்கிய நோக்கம் சர்வதேச அளவில் இ-காமர்ஸ் தொடர்பான சட்டத்தில் ஒரே சீரான தன்மையைக் கொண்டிருப்பதும், காகித அடிப்படையிலான தகவல்களுக்கும் மற்றும் மின்னணு தகவல்களுக்கும் சமமான தீர்வை வழங்குவதும் ஆகும். இந்த மாதிரிச் சட்டத்தில் இந்தியாவும் கையெழுத்திட்டுள்ளது. எனவே, தகவல் தொழில்நுட்பச் சட்டம், 2000 ஐ இயற்றியது.

E-கையொப்பம் மீதான மாதிரி சட்டம், 2001 (MLES) - 2001 ஆம் ஆண்டில், E- கையொப்பம் பற்றிய மாதிரி சட்டம் சர்வதேச வர்த்தகம் மற்றும் சட்டத்திற்கான ஐக்கிய நாடுகள் ஆணையத்தால் (UNCITRAL) ஏற்றுக்கொள்ளப்பட்டது. மின்னணு மற்றும் கையால் எழுதப்பட்ட கையொப்பங்களுக்கு இடையில் சமத்துவத்திற்கான தொழில்நுட்ப நம்பகத்தன்மையின் அளவுகோகளை நிறுவுவதன் மூலம் மின்னணு பயன்பாட்டை இயக்கி எளிதாக்குவதை நோக்கமாகக் கொண்டது. மின்னணு கையொப்பங்களை திறம்பட கையாள்வதற்கும் அவற்றின் அந்தஸ்திற்கு உறுதியளிப்பதற்கும் ஒரு நவீன, இணக்கமான மற்றும் நியாயமான சட்டமன்ற கட்டமைப்பை நிறுவுவதில் இந்த சட்டம் நாடுகளுக்கு உதவக்கூடும். அதன்படி, தகவல் தொழில்நுட்ப (திருத்தம்) சட்டம், 2008 ஐ இந்தியா நிறைவேற்றியது, இது 2000 ஆம் ஆண்டின் சட்டத்தில் தேவையான திருத்தங்களை செய்தது.

சர்வதேச ஒப்பந்தங்களில் மின்னணுவியல் தொடர்புகளைப் பயன்படுத்துவது பற்றிய ஐக்கிய நாடுகள் சபையின் மாநாடு, 2005 - இது 2005 நவம்பர் 23 இல் ஏற்றுக்கொள்ளப்பட்டு 1 மார்ச் 20 13 அன்று நடைமுறைக்கு வந்தது. உள்நாட்டிலும் சர்வதேச அளவிலும் வர்த்தகம் மற்றும் பொருளாதார அபிவிருத்தியை ஊக்குவிப்பதில் மின்னணுவியல் தொடர்புகள் ஒரு அடிப்படைப் பாத்திரத்தை வகிப்பதோடு வர்த்தக நடவடிக்கைகளின் வினைத்திறனையும் மேம்படுத்துகின்றன என்ற உண்மையை அது அங்கீகரித்துள்ளது. வெவ்வேறு சட்ட,

சமூக மற்றும் பொருளாதார நிலைகளில் மாநிலங்களால் ஏற்றுக்கொள்ளக்கூடிய வகையில் மின்னணு தகவல்தொடர்புகளைப் பயன்படுத்துவதில் உள்ள சட்டத் தடைகளை நீக்குவதற்கான ஒரு பொதுவான தீர்வை வழங்குவதை இது நோக்கமாகக் கொண்டுள்ளது. மின்னணு தொடர்பியல் ஒப்பந்தங்கள் முடிவடைந்து ஏனைய தொடர்பியல் மாநாடு உடன்படிக்கையை சர்வதேச வர்த்தகத்தில் பரிமாறிக் கொள்ளப்படுவதை உறுதிப்படுத்துவதன் மூலம், பாரம்பரிய காகித அடிப்படையிலான தகவல் பரிமாற்றத்துக்கு சமமானவற்றைப் போலவே மின்னணு முறையில் அனுப்புவது செல்லுபடியாகும் மற்றும் செயல்படுத்தக்கூடியவை என வசதியளிப்பதை நோக்கமாகக் கொண்டுள்ளது.

11.3.2 தேசிய சட்டம்

இ-காமர்ஸ் தொடர்பான UNICITRAL சட்டத்தில் இந்திய அரசு கையெழுத்திட்டு, 2000 ஆம் ஆண்டு இயற்றப்பட்டது, இது 2008 ஆம் ஆண்டில் திருத்தப்பட்ட UNICITRAL மாதிரிச் சட்டம் (மின்னணு கையெழுத்து), 2001-ஐ செயல்படுத்துவதற்காக திருத்தப்பட்டது. கணினிகள் மற்றும் தொழில்நுட்பத்தின் பயன்பாடு அல்லது உதவியுடன் அல்லது அதன் மூலம் செய்யக்கூடிய பல பாரம்பரிய குற்றங்கள் வழக்கமான குற்றங்களின் வரையறைக்குள் கொண்டுவரப்பட்டுள்ளன, எனவே திருத்தப்பட்ட 1860 ஆம் ஆண்டின் இந்திய தண்டனைச் சட்டத்தின் வரம்பிற்குள் வருகின்றன. 1872ஆம் ஆண்டு இந்தியச் சான்றுகள் சட்டத்தின் 65அ பிரிவும், 1872ஆம் ஆண்டு இந்தியச் சான்றுகள் சட்டத்தின் பிரிவு 65 பி பிரிவும் திருத்தப்பட்டு, மின்னணுப் பதிவுகளை ஆதாரமாக ஏற்றுக் கொள்ள வகை செய்கின்றன. 1891ஆம் ஆண்டு பேங்கர்ஸ் புக் எவிடன்ஸ் சட்டம் மற்றும் 1934ஆம் ஆண்டு இந்திய ரிசர்வ் வங்கிச் சட்டம் ஆகியவையும் கீழ்க்கண்டவற்றுக்குச் சான்றுகளைச் சேகரிப்பதற்கு வசதியாகத் திருத்தப்பட்டுள்ளன. அதாவது, இணைய வழிக் குற்றங்கள் அல்லது அத்தகைய குற்றங்களுடன் தொடர்புடைய எந்தவொரு விஷயத்தையும் கையாளுதல். இத்திருத்தங்களின் முக்கிய நோக்கம் மின்னணு வர்த்தகம், மின்னணு குற்றங்கள் மற்றும் சாட்சியங்கள் தொடர்பான பிரச்சினைகளை நிவர்த்தி செய்வதும் மின்னணு நிதி பரிமாற்றம் தொடர்பாக மேலதிக ஒழுங்குவிதிகளை அமுல்படுத்துவதும் ஆகும்.

மேலும் விரிவான தகவல்களுக்கு, சர்வதேச வர்த்தக சட்டம்

குறித்த ஐக்கிய நாடுகள் ஆணையத்தின் வலைத்தளத்தை நீங்கள் பார்வையிடலாம்: www.unicitral.org.

11.4 தகவல் தொழில்நுட்பச் சட்டம், 2000 திருத்தப்பட்டபடி

தகவல் தொழில்நுட்பச் சட்டம், 2000, மின்னணு தரவு பரிமாற்றம் மற்றும் பொதுவாக "மின்னணு வணிகம்" என்று குறிப்பிடப்படும் தகவல்தொடர்புகளின் பிற வழிமுறைகள் மூலம் மேற்கொள்ளப்படும் பரிவர்த்தனைகளுக்கு சட்டப்பூர்வ அங்கீகாரத்தை வழங்குவதை நோக்கமாகக் கொண்டுள்ளது, இது காகிதத்திற்கு மாற்றுகளைப் பயன்படுத்துவதை உள்ளடக்கியது. அரசாங்க முகவர்களுடன் ஆவணங்களை மின்னணு முறையில் தாக்கல் செய்வதற்கு வசதியளிப்பதற்கு வசதியாக, தகவல் தொடர்பு மற்றும் தகவல்களைச் சேமிப்பதற்கான அடிப்படையிலான முறைகள் வசதி செய்யப்பட்டுள்ளது.

11.4.1 இ-கையொப்பம் மற்றும் மின்னணு பதிவுகள்

தகவல் தொழில்நுட்பச் சட்டத்தின் பிரிவு 3A, சந்தாதாரர் ஒருவர் அத்தகைய மின்னணு கையொப்பம் அல்லது மின்னணு அங்கீகார நுட்பத்தின் மூலம் எந்தவொரு மின்னணு பதிவையும் அங்கீகரிக்கலாம் என்று வழங்குகிறது, இது (அ) நம்பகமானதாகக் கருதப்படுகிறது; மற்றும் (ஆ) இரண்டாவது அட்டவணையில் குறிப்பிடப்படலாம்.

இச்சட்டத்தின் III ஆம் அத்தியாயம் மின்னணு பதிவுகள் (பிரிவு 4), இ-கையொப்பம் (பிரிவு 5) மற்றும் அரசாங்கத்திலும் அதன் முகவர் நிலையங்களிலும் (பிரிவு 6) அவற்றின் பாவனைக்கு சட்ட அங்கீகாரம் தொடர்பானதாகும். அத்தியாயம் 4 மின் பதிவேட்டின் பண்புக்கூறு, அதன் ஒப்புகையின் முறை மற்றும் அனுப்பும் நேரம் மற்றும் இடம் மற்றும் மின்னணு பதிவுகளைப் பெறுவதற்கான நேரத்தையும் இடத்தையும் தீர்மானிப்பதற்கான விதிகளை வகுக்கிறது. பிரிவு 10A மின்னணு வழிகளில் உருவாக்கப்பட்ட ஒப்பந்தங்களில் செல்லுபடியாகும் தன்மையை வழங்குகிறது. ஐந்தாம் அத்தியாயம் பாதுகாப்பான மின்னணு பதிவுகள் மற்றும் பாதுகாப்பான மின்னணு கையொப்பத்திற்கான நிபந்தனைகளை வரையறுக்கிறது.

11.4.2 சான்றளிக்கும் அதிகாரிகளை ஒழுங்குபடுத்துதல்

சான்றுப்படுத்தல் அதிகாரசபைகளை ஒழுங்குபடுத்துவது தொடர்பான ஏற்பாடுகள் தகவல் தொழினுட்பச் சட்டத்தின் VI ஆம் அத்தியாயத்தில் கொடுக்கப்பட்டுள்ளன. அத்தியாயம் VI கட்டுப்பாட்டாளர் மற்றும் ஏனைய உத்தியோகஸ்தர்களை நியமித்தல், கட்டுப்பாட்டாளரின் தொழிற்பாடுகள், வெளிநாட்டு அத்தாட்சிப்படுத்தும் அதிகாரிகளை அங்கீகரித்தல், இ-கையொப்பச் சான்றிதழ்களை வழங்குவதற்கான அனுமதிப்பத்திரம் - விண்ணப்பம், புதுப்பித்தல், அனுமதிப்பத்திரத்தை இடைநிறுத்துதல் மற்றும் உரிமத்தை வழங்குதல் அல்லது நிராகரித்தல் நடைமுறைகள் என்பனவற்றைப் பற்றி விவரிக்கிறது.

கட்டுப்பாட்டாளரின் பணிகள்

சான்றிதழ் அதிகாரத்தின் கட்டுப்பாட்டாளர் (Controller of Certification authority) என்பது தகவல் தொழில்நுட்பச் சட்டத்தின் மையப் புள்ளியாகும், அவர் இந்தச் சட்டத்தின் கீழ் செயல்பாடுகளை மத்திய அரசின் பொதுவான கட்டுப்பாடு மற்றும் வழிகாட்டுதல்களுக்கு உட்பட்டு நிறைவேற்றுவார். தகவல் தொழில்நுட்பத்தின் பிரிவு 18 இன் படி சட்டம், கட்டுப்பாட்டாளர் பின்வரும் செயல்பாடுகளில் அனைத்தையும் அல்லது ஏதேனும் ஒன்றைச் செய்யலாம்:

a) சான்றளிக்கும் அதிகாரிகளின் செயல்பாடுகள் மீது மேற்பார்வை செய்தல்.

b) சான்றளிக்கும் அதிகாரிகளின் பொது விசைகளை சான்றளித்தல்.

c) சான்றளிக்கும் அதிகாரிகளால் பராமரிக்கப்பட வேண்டிய தரநிலைகளை வகுத்தல்.

d) சான்றளிக்கும் அதிகாரிகளின் பணியாளர்கள் பெற்றிருக்க வேண்டிய தகுதிகள் மற்றும் அனுபவத்தைக் குறிப்பிடுதல்.

e) சான்றளிக்கும் அதிகாரிகள் தங்கள் வணிகத்தை நடத்த வேண்டிய நிபந்தனைகளைக் குறிப்பிடுதல்.

f) டிஜிட்டல் கையொப்பச் சான்றிதழ் மற்றும் பொது விசையைப் பொறுத்து விநியோகிக்கப்படும் அல்லது பயன்படுத்தப்படும் எழுதப்பட்ட, அச்சிடப்பட்ட அல்லது காட்சிப் பொருட்கள் மற்றும் விளம்பரங்களின்

உள்ளடக்கங்களைக் குறிப்பிடுதல்.

g) டிஜிட்டல் கையொப்ப சான்றிதழின் வடிவம் மற்றும் உள்ளடக்கம் மற்றும் சாவியைக் குறிப்பிடுதல்.

h) சான்றளிக்கும் அதிகாரிகளால் கணக்குகள் பராமரிக்கப்படும் படிவம் மற்றும் முறையைக் குறிப்பிடுதல்.

i) தணிக்கையாளர்கள் நியமிக்கப்பட வேண்டிய விதிமுறைகள் மற்றும் நிபந்தனைகள் மற்றும் அவர்களுக்கு வழங்கப்படும் ஊதியம் ஆகியவற்றைக் குறிப்பிடுதல்.

j) மற்ற சான்றளிக்கும் அதிகாரிகளுடன் தனியாகவோ அல்லது கூட்டாகவோ சான்றளிக்கும் அதிகாரியால் எந்தவொரு மின்னணு அமைப்பையும் நிறுவுதல் மற்றும் அத்தகைய அமைப்புகளை ஒழுங்குபடுத்துதல்.

k) சான்றளிக்கும் அதிகாரிகள் சந்தாதாரர்களுடன் தங்கள் பரிவர்த்தனைகளை நடத்தும் விதத்தைக் குறிப்பிடுதல்.

l) சான்றளிக்கும் அதிகாரிகளுக்கும் சந்தாதாரர்களுக்கும் இடையே உள்ள ஏதேனும் முரண்பாடுகளைத் தீர்ப்பது.

m) சான்றளிக்கும் அதிகாரிகளின் கடமைகளை வகுத்தல்.

n) ஒவ்வொரு சான்றளிக்கும் ஆணையத்தின் வெளிப்படுத்தல் பதிவைக் கொண்ட தரவுத் தளத்தைப் பராமரித்தல், விதிமுறைகளால் குறிப்பிடப்படும், அவை பொதுமக்களுக்கு அணுகக்கூடியதாக இருக்கும்.

கட்டுப்பாட்டாளரின் அதிகாரங்கள்

அனுமதிப்பத்திரத்தை வழங்குவதற்கான அல்லது நிராகரிப்பதற்கான நடைமுறை 24 ஆம் பிரிவில் குறிப்பிடப்பட்டுள்ளது. இப்பிரிவின் பிரகாரம், கட்டுப்பாட்டாளர், பிரிவு 21(1) இன் கீழ் விண்ணப்பப் பத்திரமொன்றைப் பெற்றுக்கொண்டதன் பின்னர், விண்ணப்பப் பத்திரத்துடன் கூடிய ஆவணங்களையும், அவர் பொருத்தமெனக் கருதும் அத்தகைய ஏனைய காரணிகளையும் பரிசீலித்ததன் பின்னர் அனுமதிப்பத்திரத்தை வழங்கலாம் அல்லது விண்ணப்பத்தை நிராகரிக்கலாம். எவ்வாறாயினும், விண்ணப்பதாரர் தனது வழக்கை முன்வைப்பதற்கான நியாயமான சந்தர்ப்பம் வழங்கப்பட்டாலொழிய, இந்தப் பிரிவின் கீழ் எந்தவொரு விண்ணப்பமும் நிராகரிக்கப்படமாட்டாது.

உரிமத்தை இடைநிறுத்துவதற்கான நடைமுறை பிரிவு 25 இல்

வரையறுக்கப்பட்டுள்ளது. இந்தப் பிரிவின்படி:

1) கட்டுப்பாட்டாளர் விசாரணையைச் செய்ததன் பின்னர் திருப்தியடைந்தால், ஒரு சான்றளிக்கும் அதிகாரி பின்வருவனவற்றைக் கொண்டிருந்தால் பொருத்தமானதாக இருக்கும் என்று கருதலாம் -

a) அனுமதிப்பத்திரத்தை வழங்குவதற்கான அல்லது புதுப்பித்தலுக்கான விண்ணப்பம் பொருள் விபரங்களில் தவறானது அல்லது தவறானது என அறிக்கையொன்றை சமர்ப்பித்தல்;

b) உரிமம் வழங்கப்பட்ட விதிமுறைகள் மற்றும் நிபந்தனைகளுக்கு இணங்கத் தவறியது;

c) பிரிவு 30 இல் குறிப்பிடப்பட்டுள்ள நடைமுறைகள் மற்றும் தரத்தைப் பேணத் தவறியது;

d) இச்சட்டத்தின் ஏதேனும் ஏற்பாடுகள், அதன் விதிகள், ஒழுங்குவிதிகள் அல்லது கட்டளைகள் என்பவற்றை மீறுதல்; உரிமத்தைத் திரும்பப் பெறுதல்: முன்மொழியப்பட்ட திரும்பப்பெறுதலுக்கு எதிராக காரணத்தைக் காண்பிப்பதற்கான நியாயமான வாய்ப்பு சான்றளிக்கும் அதிகாரசபைக்கு வழங்கப்பட்டாலொழிய, எந்தவொரு உரிமமும் இரத்துச் செய்யப்பட மாட்டாது.

2) கட்டுப்பாட்டாளர், மேற்குறிப்பிட்ட உபபிரிவு (1) இன் கீழ் உரிமத்தை இரத்துச் செய்வதற்கு ஏதேனும் முகாந்திரம் இருப்பதாக நம்புவதற்கு நியாயமான காரணங்கள் இருப்பின், அவர் கட்டளையிட்ட எந்தவொரு விசாரணையையும் முடிக்கும் வரை, அத்தகைய உரிமத்தை இடைநிறுத்தலாம். எவ்வாறாயினும், உத்தேச இடைநிறுத்தத்திற்கு எதிராக காரணத்தைக் காண்பிப்பதற்கான நியாயமான சந்தர்ப்பம் அத்தாட்சிப்படுத்தும் அதிகாரசபைக்கு வழங்கப்பட்டாலொழிய, பத்து நாட்களுக்கு மேல் எந்தவொரு அனுமதிப்பத்திரமும் இடைநிறுத்தப்படமாட்டாது.

3) அனுமதிப்பத்திரம் இடைநிறுத்தப்பட்டுள்ள காலத்தில் எந்தவொரு சான்றையும் வழங்காது.

இச்சட்டத்தின் 28 மற்றும் 29 ஆம் பிரிவுகள், கட்டுப்பாட்டாளர் அல்லது அவரால் அதிகாரமளிக்கப்பட்ட எந்தவொரு அலுவலருக்கும் விதிமீறல்களை விசாரிப்பதற்கும், கணினிகள் மற்றும் தரவுகளை அணுகுவதற்கும் இச்சட்டத்தின் விதிகள்

அல்லது ஒழுங்குவிதிகள் அதிகாரத்தை வழங்குகின்றன.

11.4.3 சைபர் மேல்முறையீட்டு தீர்ப்பாயம்

தகவல் தொழில்நுட்பச் சட்டத்தின் பிரிவு 57 இணையதள மேல்முறையீட்டு தீர்ப்பாயத்திற்கு மேல்முறையீடு செய்வது தொடர்பான விதிகளை வகுக்கிறது.

- இச்சட்டத்தின் கீழ் கட்டுப்பாட்டாளர் அல்லது ஒரு தீர்ப்பு அதிகாரியால் பிறப்பிக்கப்பட்ட உத்தரவினால் பாதிக்கப்பட்ட எவரும், மேற்சொன்ன உத்தரவின் நகல் கிடைத்த நாற்பத்தைந்து நாட்களுக்குள், இந்த விஷயத்தில் அதிகார வரம்பைக் கொண்ட இணையதள மேல்முறையீட்டு தீர்ப்பாயத்தில் மேல்முறையீடு செய்யலாம். எவ்வாறாயினும், இரு தரப்பினரின் ஒப்புதலுடன் ஒரு தீர்ப்பு அதிகாரியால் பிறப்பிக்கப்பட்ட உத்தரவிலிருந்து இணையதள மேல்முறையீட்டு தீர்ப்பாயத்திற்கு மேல்முறையீடு செய்யக்கூடாது. இணையதள மேல்முறையீட்டு தீர்ப்பாயம் நாற்பத்தைந்து நாட்கள் முடிந்த பிறகு, அந்த காலத்திற்குள் தாக்கல் செய்யாததற்கு போதுமான காரணம் இருப்பதாக திருப்தி அடைந்தால், மேல்முறையீடு செய்யலாம்.
- இணையதள மேல்முறையீட்டு தீர்ப்பாயம் இரு தரப்பினருக்கும் மேல்முறையீட்டிற்கு இடமளிக்கும், அத்தகைய உத்தரவுகளை பிறப்பிக்கும் முன் விசாரிக்கப்படுவதற்கான வாய்ப்பை வழங்கும்.
- இணையதள மேல்முறையீட்டுத் தீர்ப்பாயத்தில் தாக்கல் செய்யப்படும் மேல்முறையீடு, மேல்முறையீடு பெறப்பட்ட தேதியிலிருந்து ஆறு மாதங்களுக்குள் இறுதித் தீர்வுக்கான முயற்சியுடன் கூடிய விரைவில் முடிக்கப்படும்.

இணையதள மேல்முறையீட்டு தீர்ப்பாயத்தின் நடைமுறை மற்றும் அதிகாரங்கள் - தகவல் தொழில்நுட்பச் சட்டத்தின் பிரிவு 58, இணையதள மேல்முறையீட்டு தீர்ப்பாயம் அதன் செயல்பாடுகளை நிறைவேற்றும் நோக்கங்களுக்காக, ஒருவரிடம் வழங்கப்பட்டுள்ள அதே அதிகாரங்களைக் கொண்டுள்ளது என்று வழங்குகிறது. சிவில் நடைமுறைச் சட்டம், 1908 இன் கீழ் சிவில் நீதிமன்றம் வழக்கை விசாரிக்கும் போது. எவ்வாறாயினும், 1908 ஆம் ஆண்டு உரிமையியல் நடைமுறைச் சட்டக்கோவையின் 5 ஆம் பிரிவினால் வரையறுக்கப்பட்டுள்ள நடைமுறைகளுக்கு தீர்ப்பாயம் கட்டுப்படாது, மாறாக பின்வரும்

கொள்கைகளின்படி வழிநடத்தப்படுதல் வேண்டும். இயற்கை நீதி மற்றும், இந்த தகவல் தொழில்நுட்பச் சட்டம் மற்றும் அதன் விதிகளின் பிற விதிகளுக்கு உட்பட்டது. தீர்ப்பாயம் அதன் அமர்வுகளைக் கொண்ட இடம் உட்பட அதன் சொந்த நடைமுறையை ஒழுங்குபடுத்தும் அதிகாரங்களைக் கொண்டிருக்கும்.

11.4.4 இடைத்தரகர்கள்

தகவல் தொழில்நுட்பச் சட்டத்தின் பிரிவு 2 (1) (w) வரையறுக்கிறது: இடைத்தரகர் என்பது மற்றொரு நபரின் சார்பாக ஸ்டோர்களைப் பெறும் அல்லது அந்த பதிவை அனுப்பும் அல்லது அந்த பதிவு தொடர்பான எந்தவொரு சேவையையும் வழங்கும் எந்தவொரு நபரையும் குறிக்கிறது. இடைத்தரகர் பின்வருவனவற்றை உள்ளடக்குகிறது: தொலைத்தொடர்பு சேவை வழங்குநர்கள்; நெட்வொர்க் சேவை வழங்குநர்கள்; இணைய சேவை வழங்குநர்கள்; வலை ஹோஸ்டிங் சேவை வழங்குநர்கள்; தேடுபொறிகள்; ஆன்லைன் கட்டணம் செலுத்தும் தளங்கள்; ஆன்லைன்- ஏல தளங்கள்; ஆன்லைன்-சந்தை இடங்கள் மற்றும் சைபர் க஻ேபக்கள்.

நாடுகள் மற்றும் பொருளாதாரத்தின் அனைத்து அம்சங்களிலும் ஊடுருவும் அளவுக்கு இணையம் வளர்ந்துள்ளது; இணையத்தில் மூன்றாம் தரப்பினருக்கு இடையிலான தொடர்புகள், பரிவர்த்தனைகள் அல்லது செயல்பாடுகளை ஒன்றிணைப்பதில் அல்லது எளிதாக்குவதில் இணைய இடைத்தரகர்களின் பங்கு முக்கியமானது, ஏனெனில் அவர்கள் ஆன்லைன் தகவல்கள் சேவைகள் மற்றும் பொருட்களுக்கு இடையிலான அணுகல் மற்றும் தேர்வை ஆதிக்கம் செலுத்துகிறார்கள், தீர்மானிக்கிறார்கள்.

இடைத்தரகர்களின் கடமைகள்:

- தகவல் தொழில்நுட்பச் சட்டத்தின் பிரிவு 67 சி இன் படி, இடைத்தரகர் அத்தகைய தகவல்களை கால அளவு, முறை மற்றும் வடிவத்தை மத்திய அரசு விதிக்கக்கூடிய வகையில் பாதுகாத்து வைத்திருக்க வேண்டும். இந்த கடமையை வேண்டுமென்றே மீறினால், இடைத்தரகர் மூன்று ஆண்டுகள் வரை சிறைத்தண்டனை மற்றும் அபராதமும் விதிக்கப்பட வேண்டும் என்று சட்டம் வகை செய்கிறது,
- பிரிவு 69(3) சந்தாதாரர் அல்லது இடைத்தரகர் அல்லது

கணினி வளத்திற்குப் பொறுப்பான எவரேனும் நபர், மத்திய அரசு அல்லது ஒரு மாநில அரசால் அல்லது சிறப்பாக அதிகாரமளிக்கப்பட்ட அதன் அதிகாரிகளால் அழைக்கப்படும்போது, மத்திய அரசோ அல்லது மாநில அரசோ அவர்களுக்கு அனைத்து வசதிகளையும் தொழில்நுட்ப உதவிகளையும் வழங்க வேண்டும். இடைத்தரகருக்கு கீழ்கண்டவற்றை அணுக வாய்ப்பு வழங்கப்படும் (அ) அத்தகைய தகவல்களை உருவாக்குதல், அனுப்புதல், பெறுதல் அல்லது சேமித்தல் ; அல்லது (ஆ) தகவலை இடைமறித்தல், கண்காணித்தல் அல்லது மறைகுறிநீக்குதல் ; அல்லது (c) கணினி ஆதாரத்தில் சேமிக்கப்பட்ட தகவல்.

- தகவல் தொழில்நுட்பச் சட்டம், எந்தவொரு கணினி வளத்தின் மூலமும் எந்தவொரு தகவலையும் பொதுமக்கள் அணுகுவதைத் தடுப்பதையும் கையாள்கிறது. இது தொடர்பாக அரசு பிறப்பித்துள்ள வழிகாட்டுதலுக்கு இடைத்தரகர் இணங்க வேண்டும். இடைத்தரகர் வழங்கப்பட்ட வழிகாட்டுதலுக்கு இணங்கத் தவறினால், ஏழு ஆண்டுகள் வரை நீட்டிக்கக்கூடிய ஒரு காலத்திற்கு சிறைத்தண்டனையும் அபராதமும் விதிக்கப்படும்.

இடைத்தரகர்களின் பங்கு மற்றும் சட்டம்

இடைத்தரகர்கள் முக்கிய பங்கு வகிக்கின்றனர் மற்றும் பயனர்கள் தகவல்களை அணுகுவதற்கும், சமூக நடவடிக்கைகள் மற்றும் குடிமக்களின் பங்கேற்புக்கு புதிய வாய்ப்புகளை வழங்குவதற்கும் உதவும் கருவிகளாக செயல்படுகிறார்கள். இணைய பாதுகாப்பு, இ-நுகர்வோர் பாதுகாப்பு மற்றும் தனியுரிமை மற்றும் அறிவுசார் சொத்துரிமைகளைப் பாதுகாப்பதன் மூலம் தீங்கு விளைவிப்பதைத் தடுப்பதற்கான அவர்களின் தொழில்நுட்ப திறன் மிகவும் முக்கியமானது. சில கடமைகள் மற்றும் பொறுப்புகளைத் தவிர இடைத்தரகர்களுக்கு பயனர்களால் சட்டவிரோத உள்ளடக்கத்தை இடுகையிடுவதன் காரணமாக எழக்கூடிய சட்டப்பூர்வ பொறுப்பிலிருந்து பாதுகாப்பு அல்லது விலக்கு வழங்கப்பட வேண்டும் என்பது உலகெங்கிலும் எப்போதும் கவலையாக இருந்து வருகிறது. அமெரிக்கா மற்றும் ஐரோப்பிய ஒன்றியத்தின் உறுப்பினர்கள் போன்ற பல நாடுகளில், அத்தகைய பயனர் உருவாக்கிய உள்ளடக்கத்திலிருந்து இடைத்தரகர்களுக்கு சட்ட பாதுகாப்பை வழங்குவதற்கான முயற்சிகள் உள்ளன. இத்தகைய பாதுகாப்பு

பெரும்பாலும் 'பாதுகாப்பான மையம்' பாதுகாப்பு என்று அழைக்கப்படுகிறது. எங்கள் தகவல் தொழில்நுட்பச் சட்டம், கீழே விவாதிக்கப்பட்டபடி சில சந்தர்ப்பங்களில் இடைத்தரகர்களின் பொறுப்பிலிருந்து விலக்கு அளிக்கவும் வகை செய்கிறது:

பொறுப்பிலிருந்து விலக்களிப்பு

தகவல் தொழில்நுட்பச் சட்டத்தின் கீழ் இடைத்தரகர்கள் பின்வரும் சந்தர்ப்பங்களில் மற்றவர்களுக்குக் கிடைக்கச் செய்யப்படும் எந்தவொரு மூன்றாம் தரப்புத் தகவல், தரவு அல்லது தகவல்தொடர்பு இணைப்புக்கும் பொறுப்பேற்க மாட்டார்கள்:

a) எங்கே இடைத்தரகர் இல்லை -

i) பரிமாற்றம் தொடங்க,

ii) டிரான்ஸ்மிஷனின் ரிசீவரைத் தேர்ந்தெடுக்கவும், மற்றும்

iii) பரிமாற்றத்தில் உள்ள தகவலைத் தேர்ந்தெடுக்கவும் அல்லது மாற்றவும்;

b) இச்சட்டத்தின் கீழ் இடைத்தரகர் தனது கடமைகளை நிறைவேற்றும் போது உரிய விடாமுயற்சியைக் கடைப்பிடிப்பதோடு, மத்திய அரசு அவ்வப்போது விதிக்கக்கூடிய பிற வழிகாட்டுதல்களையும் கடைப்பிடிக்கிறார்.

இடைத்தரகர்களின் பொறுப்பு

பின்வரும் சூழ்நிலைகளில் இடைத்தரகர் பொறுப்பேற்க வேண்டும்:

a) இடைத்தரகர் அச்சுறுத்தல்கள் அல்லது வாக்குறுதி அல்லது சட்டவிரோத செயலின் ஆணையத்தில் வேறுவிதமாக சதி அல்லது உடந்தையாக இருந்திருக்கிறார்;

b) இடைத்தரகர்களால் கட்டுப்படுத்தப்படும் ஒரு கணினி வளத்தில் இருக்கும் அல்லது அதனுடன் இணைக்கப்பட்டுள்ள எந்தவொரு தகவல், தரவு அல்லது தகவல்தொடர்பு இணைப்பும் சட்டவிரோத செயலைச் செய்ய பயன்படுத்தப்படுகிறது என்று பொருத்தமான அரசாங்கம் அல்லது அதன் நிறுவனத்தால் தெரிவிக்கப்பட்டால், இடைத்தரகர் விரைவாக அகற்றத் தவறினால் அல்லது எந்த வகையிலும் ஆதாரங்களை சிதைக்காமல் அந்த ஆதாரத்தில் அந்த

மூலப்பொருளுக்கான அணுகலை முடக்கவும்.

தன் மதிப்பீடு 2

குறிப்பு: உங்கள் பதில்களுக்கு கீழே உள்ள இடத்தைப் பயன்படுத்தவும்

உங்கள் பதில்களை இந்த பாடப் பகுதியின் இறுதியில் கொடுக்கப்பட்ட பதில்களுடன் சரிபார்த்துக் கொள்ளவும்.

1) 'இடைத்தரகர்கள்' என்ற சொல்லை வரையறுக்கவும்.

.....

.....

.....

.....

.....

.....

2) இணைய வழி மேல்முறையீட்டு தீர்ப்பாயத்தில் யார் மேல்முறையீடு செய்யலாம் ?

.....

.....

.....

.....

.....

.....

11.5 இணையதளக் குற்றங்கள்

இணையவழி குற்றங்கள் என்ற சொல் கணினிகள் மற்றும் நெட்வொர்க்குகளை உள்ளடக்கிய பரந்த அளவிலான குற்றங்களைக் குறிக்கிறது, அங்கு கணினி குற்றம் செய்வதற்கான ஒரு கருவியாகப் பயன்படுத்தப்படுகிறது அல்லது கணினியே ஒரு குற்றத்தின் இலக்காகவோ அல்லது ஒரு குற்றத்திற்கு தற்செயலாகவோ உள்ளது. இணைய வழி குற்றங்கள் என்ற சொல், பொதுவான அர்த்தத்தில் பயன்படுத்தப்பட்டால், அதன் நோக்கம் பல வகையான சிவில் மற்றும் கிரிமினல் தவறுகளை உள்ளடக்கும் வகையில் நீட்டிக்கப்படலாம். இணைய வழிக் குற்றங்கள் தனிநபர்கள் அல்லது சொத்துக்களுக்கு எதிராக செய்யப்படுகின்றன, அவை

ஒரு நிறுவனத்திற்கு எதிராகவும் செய்யப்படுகின்றன - அரசாங்கம், அரசு அல்லாத; நிறுவனம்; தனிநபர்களின் நிறுவனம் அல்லது குழு, அல்லது பெரிய அளவில் சமூகத்திற்கு எதிராக.

11.5.1 கணினி குற்றங்களின் வகைகள்

கணினி குற்றங்களை கீழே கொடுக்கப்பட்டுள்ளவாறு வகைப்படுத்தலாம்:

கணினி மூலம் செய்யப்படும் வழக்கமான குற்றங்கள்: தனிநபர்கள் மற்றும் அவர்களது உடைமைகளுக்கு எதிராக செய்யப்படும் பல பாரம்பரிய அல்லது வழக்கமான குற்றங்கள் உள்ளன. இந்த குற்றங்களில் பல இப்போது கணினிகளின் உதவியுடன் செய்யப்படுகின்றன. இணைய அவதூறு, இணைய ஆபாசம், இணைய வழி பின்தொடர்தல் / துன்புறுத்தல், ஏமாற்றுதல், டிஜிட்டல் மோசடி, திருட்டு, இணைய மோசடி / ஏமாற்றுதல், கிரெடிட் கார்டு மோசடிகள், பணமோசடி ஆன்லைன் சூதாட்டம் மற்றும் சட்டவிரோத கட்டுரைகளின் விற்பனை உள்ளிட்ட நிதி குற்றங்கள், இணைய பயங்கரவாதம் போன்றவை இந்திய தண்டனைச் சட்டம் மற்றும் தகவல் தொழில்நுட்பச் சட்டம் ஆகிய இரண்டின் கீழும் தண்டனைக்குரிய குற்றங்களாகும்.

இணையவழி அவதூறு (ஒரு வலைத்தளத்தில் ஒருவரைப் பற்றி அவதூறான அறிக்கையை வெளியிடுவது அல்லது பாதிக்கப்பட்டவரின் தெரிந்த தொடர்புகளுக்கு அவதூறான தகவல்களைக் கொண்ட மின்னஞ்சல்களை அனுப்புவது) இந்திய தண்டனைச் சட்டத்தின் (ஐபிசி) பிரிவு 499 இன் கீழ் தகவல் தொழில்நுட்ப சட்டத்தின் பிரிவு 4 உடன் படிக்கப்படுகிறது. இந்திய தண்டனைச் சட்டம் பிரிவு 420-ன் கீழ் அடங்கும். ஆவணங்களின் டிஜிட்டல் மோசடி என்பது ஒரு ஆவணத்தை உருவாக்குவதாகும், இது உண்மையானது அல்ல என்று ஒருவருக்குத் தெரியும், இன்னும் அது உண்மையானது என்பதைப் போலவே திட்டமிடுகிறது. மோசடியான பிறப்புச் சான்றிதழ்கள், அடையாள அட்டைகள் போன்றவை ஐபிசி மற்றும் தகவல் தொழில்நுட்பச் சட்டத்தின் பல்வேறு பிரிவுகளுடன் கையாளப்படுகின்றன. இணைய தளத்தை பின்தொடர்தல், அதாவது இணைய தளம், மின்னஞ்சல் அல்லது பிற மின்னணு தகவல்தொடர்பு சாதனங்களின் உதவியுடன் பாதிக்கப்பட்டவரைக் குறிவைத்து மற்றொரு நபரைத் துரத்துவதற்காக குற்றவாளியின் துன்புறுத்தல் அல்லது அச்சுறுத்தும் நடத்தையின்

தொடர்ச்சியான செயல்கள் ஐ.பி.சி.யின் கீழ் ஒரு இணையவழிக் குற்றமாகும். இணைய ஆபாசம், பாலியல் செயல்களைக் காட்டுவது ஆகியவை ஐபிசி பிரிவுகள் 292 மற்றும் 293, பிரிவுகள் 67,67 ஏ மற்றும் 67 பி தகவல் தொழில்நுட்ப சட்டம் மற்றும் பெண்களின் அநாகரிகமான பிரதிநிதித்துவச் சட்டம் ஆகியவற்றின் கீழ் கையாளப்படலாம்.

ஒரு கணினி நெட்வொர்க்கில் செய்யப்பட்ட குற்றங்கள் மற்றும் அஞ்சல் தொடர்பான குற்றங்கள்: இந்த குற்றங்கள் ஹேக்கிங் / அங்கீகரிக்கப்படாத அணுகல், மின்னஞ்சல் ஸ்பேமிங் அல்லது மின்னஞ்சல் ஸ்பூ஼பிங் போன்ற தொழில்நுட்பத்தால் இயக்கப்படும் குற்றங்களாகும். கணினி அமைப்பு மற்றும்/அல்லது நெட்வொர்க்கில் சட்டவிரோத ஊடுருவலை ஸ்பேமிங் செய்யும் மின்னஞ்சல் ஸ்பேமிங். மின்னஞ்சல் ஸ்பேமிங் என்பது பாதிக்கப்பட்டவர்களுக்கு அதிக அளவு அஞ்சல்களை அனுப்புவதைக் குறிக்கிறது, இதன் விளைவாக அவர்களின் கணக்கு அல்லது அஞ்சல் சேவையகம் செயலிழக்கிறது. மின்னஞ்சல் ஸ்பூ஼பிங் என்பது ஒரு மின்னஞ்சலைக் குறிக்கிறது, இது ஒரு மூலத்திலிருந்து தோன்றியதாகத் தோன்றுகிறது, இருப்பினும் அது உண்மையில் மற்றொரு மூலத்திலிருந்து அனுப்பப்பட்டுள்ளது. இக்குற்றங்கள் இந்திய தண்டனைச் சட்டம் மற்றும் தகவல் தொழில்நுட்பச் சட்டத்தின் கீழ் கையாளப்படுகின்றன.

தரவு மாற்றம் / அழிவு தொடர்பான குற்றங்கள்: கணினி நாசவேலை, வைரஸ் / புழுக்கள் / ட்ரோஜன் குதிரைகள் / ட்ரோஜன் குதிரைகள் / லாஜிக் குண்டு பரவுதல், இணைய மணிநேர திருட்டு; தரவு டிட்லிங், சலாமி தாக்குதல்கள்- வாடிக்கையாளர்களின் கணக்கில் அற்பமான மாற்றம், இது ஒரு விஷயத்தில் முற்றிலும் கவனிக்கப்படாமல் போகும்; ஃபிஷிங், முதலியன. தரவு டிட்லிங் என்பது ஒரு வகையான இணைய வழி குற்றமாகும். இதில் தரவு ஒரு கணினி அமைப்பில் உள்ளிடப்படும்போது, பெரும்பாலும் ஒரு தரவு நுழைவு எழுத்தர் அல்லது கணினி வைரஸால் தரவு மாற்றப்படுகிறது. ஃபிஷிங் என்பது உள்நுழைவு நற்சான்றுகள் மற்றும் கிரெடிட் கார்டு எண்கள் உள்ளிட்ட பயனர் தரவைத் திருட பெரும்பாலும் பயன்படுத்தப்படும் ஒரு வகையான இணையவழி குற்றமாகும். பொதுவாக இது சில நம்பகமான நிறுவனத்தின் மாறுவேடத்தின் கீழ் ஒரு நபரால் செய்யப்படுகிறது.

தகவல் தொழில்நுட்ப சட்டத்தின் பிரிவு 43 சிவில்

பொறுப்பையும் வழங்குகிறது.

அறிவுசார் சொத்துரிமை மீறல் தொடர்பான குற்றங்கள் - எடுத்துக்காட்டுகள் திருட்டு மென்பொருள் விநியோகம்; மற்றும் இணையவழி ஸ்குவாட்டிங் அதாவது உரிமையாளரின் தனித்துவமான வர்த்தக முத்திரையைக் கொண்ட ஒரு டொமைன் பெயரைப் பெறுதல். அறிவுசார் சொத்துக்களை பாதுகாப்பதற்கான பாரம்பரிய சட்டங்களும் டிஜிட்டல் ஊடகங்களில் நடக்கும் மீறல்களுக்கும் பொருந்தும்.

11.5.2 இணையதளக் குற்றங்கள்: சில வழக்குகள்

போலி அடையாளம், அவதூறு, ஏமாற்றுதல் மற்றும் இணைய வழி ஆபாசம், வெளியிடுதல் அல்லது ஆபாசமான பொருள்களை மின்னணு வடிவில் கடத்துதல் ஆகியவற்றைக் கையாளும் இணைய வழிக் குற்றங்கள் தொடர்பான சில வழக்குகளைப் பற்றி நீங்கள் தெரிந்துகொள்வது உங்களுக்கு பயனுள்ளதாக இருக்கும்.

SMC நியூமேடிக்ஸ் (இந்தியா) பிரைவேட் லிமிடெட். லிமிடெட். எதிர் ஜோகேஷ் க்வாத்ரா, 12 பிப்ரவரி 20 14 அன்று டெல்லி ஏ.டி.ஜே.யால் முடிவு செய்யப்பட்டது

இந்த வழக்கில் பிரதிவாதி ஜோகேஷ் குவாத்ரா வாதி நிறுவனத்தின் ஊழியராக இருப்பதால், அவரது முதலாளிகளுக்கும் உலகெங்கிலும் உள்ள நிறுவனத்தின் பல்வேறு துணை நிறுவனங்களுக்கும், நிறுவனத்தையும் அதன் நிர்வாக இயக்குநரையும் இழிவுபடுத்தும் நோக்கத்துடன் தரக்குறைவான, அவதூறான, ஆபாசமான, அசிங்கமான மற்றும் மோசமான மின்னஞ்சல்களை அனுப்பியதாக குற்றம் சாட்டப்பட்டது.. பிரதிவாதி மேற்குறிப்பிட்ட சட்டவிரோத செயல்களைச் செய்வதைத் தடுக்கும் வகையில் நிரந்தரத் தடையுத்தரவிற்காக வாதி ஒரு வழக்கைத் தாக்கல் செய்தார். தில்லி உயர் நீதிமன்றத்தின் மாண்புமிகு நீதிபதி, வாதியால் ஒரு முகாந்திரமான வழக்கு முன்வைக்கப்பட்டிருப்பதாகவும், அதன் விளைவாக பிரதிவாதி இழிவான, அவதூறான செய்திகளை அனுப்புவதைத் தடுத்ததாகவும் கூறி இடைக்காலத் தடையுத்தரவு ஒன்றை பிறப்பித்தார். ஆபாசமான, கொச்சையான, அவமானகரமான மற்றும் தவறான மின்னஞ்சல்கள் வாதிகளுக்கோ அல்லது உலகெங்கிலும் உள்ள அதன் துணை நிறுவனங்களுக்கோ அவற்றின் நிர்வாக இயக்குநர்கள் மற்றும் அவற்றின் விற்பனை மற்றும் சந்தைப்படுத்தல் துறைகள் உட்பட.

பிரதிவாதி மேலும் உண்மையான உலகில் மற்றும் சைபர்ஸ்பேஸ் ஆகியவற்றில் எந்தவொரு தகவலையும் வெளியிடுவதிலிருந்தும், அனுப்புவதிலிருந்தும் அல்லது வெளியிடுவதிலிருந்தும் தடுக்கப்பட்டார், இது வாதிகளை இழிவுபடுத்தும் அல்லது அவதூறாக அல்லது துஷ்பிரயோகம் செய்கிறது.

எவ்வாறாயினும், ஏடிஜே, டெல்லி 12 பிப்ரவரி 2014 தேதியிட்ட தீர்ப்பில், "இந்த நீதிமன்றம் இந்த மின்னஞ்சல்களை குறிப்பாக பிரதிவாதிதான் அனுப்புகிறார் என்று ஊகிக்க நேரடி ஆதாரங்கள் இல்லாத சூழ்நிலையில் வாதியின் சார்பாக வலுவான வாதத்தை ஏற்றுக்கொள்ளும் நிலையில் இல்லை - சமநிலையின் சோதனை நிகழ்தகவுகள் பதிவேட்டில் உள்ள சான்றுகளுக்கு பயன்படுத்தப்பட வேண்டும், அனுமானங்களுக்கு அல்ல". அதன்படி இந்த பிரச்சினை வாதிகளுக்கு எதிராக முடிவு செய்யப்பட்டு பிரதிவாதிக்கு ஆதரவாகவும், வாதியின் வழக்கு தள்ளுபடி செய்யப்பட்டது.

தமிழ்நாடு எதிர் சுஹாஸ் கட்டி, ஏ.எம்.எம் நீதிமன்றம், எழும்பூர் (2004 ஆம் ஆண்டின் சி.சி.எண் 4680)

இது 2000 ஆம் ஆண்டின் பிரிவு 67 இன் கீழ் இந்தியாவில் முதல் தண்டனையாக கருதப்படுகிறது. இந்த வழக்கில் குற்றம் சாட்டப்பட்டவர், பாதிக்கப்பட்டவரின் அறியப்பட்ட குடும்ப நண்பர் அவளை திருமணம் செய்து கொள்ள ஆர்வமாக இருந்தார். இருப்பினும், பாதிக்கப்பட்டவர் மற்றொரு நபரை திருமணம் செய்து கொண்டார், அந்த திருமணம் பின்னர் விவாகரத்தில் முடிந்தது. குற்றம் சாட்டப்பட்டவர் அவளை மீண்டும் தொடர்பு கொள்ளத் முயன்றார், ஆனால் அவர் அவரது திருமண முன்மொழிவை நிராகரித்தார். குற்றம் சாட்டப்பட்டவர் யாஹூ செய்திக் குழுவில் ஆபாசமான, அவதூறான மற்றும் எரிச்சலூட்டும் செய்தியை இடுகையிடுவதன் மூலம் இணையம் மூலம் பாதிக்கப்பட்டவரை துன்புறுத்தினார், பாதிக்கப்பட்டவரின் பெயரில் அவரால் திறக்கப்பட்ட ஒரு தவறான மின்னஞ்சல் கணக்கின் மூலம் பாதிக்கப்பட்டவருக்கு மின்னஞ்சல்கள் அனுப்பினார். இந்த செய்தியை இடுகையிடுவதன் விளைவாக பல நபர்களிடமிருந்து பாதிக்கப்பட்டவருக்கு செய்திகள் மற்றும் தொலைபேசி அழைப்புகள் வந்தன, மேலும் அவர் பாலியல் தொழிலுக்காக விரும்புவதாக நம்பும் நபர்களிடமிருந்து தொலைபேசி அழைப்புகளையும் பெற்றார்.

குற்றம் சாட்டப்பட்டவர், தகவல் தொழில்நுட்ப சட்டம் 2000

இன் பிரிவு 67 மற்றும் இந்திய தண்டனைச் சட்டத்தின் 469, 509 இன் கீழ் குற்றம் நிரூபிக்கப்பட்டு தண்டனை விதிக்கப்பட்டார். இந்த தண்டனையில் இரண்டு ஆண்டுகள் சிறைத்தண்டனை மற்றும் அபராதம் ஆகியவை அடங்கும்.

நேஷனல் அசோசியேஷன் ஆ◌ஃப் சாப்ட்வேர் (நாஸ்காம்), எதிர் அஜய் சூட் மற்றும் பலர், மார்ச் 2005 அன்று தில்லி உயர் நீதிமன்றத்தால் முடிவு செய்யப்பட்டது.

இந்த வழக்கில் பிரதிவாதிகள் ஆள் தேடுதல் மற்றும் ஆட்சேர்ப்பு ஆகியவற்றில் ஈடுபட்டுள்ள ஒரு வேலை வாய்ப்பு நிறுவனத்தை நடத்தி வந்தனர். தனிப்பட்ட தரவுகளைப் பெறுவதற்காக, அவர்கள் சிலரை தேர்ந்தெடுத்து வேலை வாய்ப்பு வழங்கும் நோக்கங்களுக்காகப் பயன்படுத்தக்கூடிய வகையில், பிரதிவாதிகள் நாஸ்காம் என்ற பெயரில் மூன்றாம் தரப்பினருக்கு மின்னஞ்சல்களை எழுதி அனுப்பினர். பிரதிவாதிகள் அல்லது அவர்களின் கீழ் செயல்படும் எந்தவொரு நபரையும் தடுக்கும் நிரந்தர தடையுத்தரவு பிறப்பிக்கப்பட வேண்டும் என்று கோரி மனுதாரர் வழக்கைத் தாக்கல் செய்தார்

வர்த்தகக் குறியான 'நாஸ்காம்' அல்லது சரக்குகள் அல்லது சேவைகள் தொடர்பாக குழப்பமான வகையில் ஒத்த வேறு எந்த அடையாளத்தையும் பயன்படுத்திய வாதியிடமிருந்து தோன்றியதாகக் கூறப்படும் மோசடி மின்னஞ்சல்களை புழக்கத்தில் இருந்து வரும் அதிகாரம், சேதங்களுக்கான இழப்பு கோருதல் வெளிப்படையாக நடந்தது.

மார்ச் 23, 2005 அன்று வழங்கப்பட்ட இந்த வரலாற்றுச் சிறப்புமிக்க தீர்ப்பு, குறிப்பிட்ட சட்டங்கள் இல்லாத நிலையிலும் கூட இந்தியச் சட்டங்களின் வரம்பிற்குள் "◌ஃபிஷிங்" என்ற செயலைக் கொண்டுவருகிறது. "இந்திய சட்டத்தின் கீழ் ◌ஃபிஷிங்கிற்கு சமமான ஒரு செயல், வர்த்தகத்தின் போது செய்யப்படும் ஒரு தவறான விளக்கமாக இருக்கும், இது மின்னஞ்சலின் ஆதாரம் மற்றும் தோற்றம் குறித்து குழப்பத்திற்கு வழிவகுக்கும், இது நுகர்வோருக்கு மட்டுமல்லாமல், பெயர், அடையாளம் அல்லது கடவுச்சொல் தவறாகப் பயன்படுத்தப்படும் நபருக்கும் கூட பெரும் தீங்கு விளைவிக்கும். பாதிக்கப்பட்ட தரப்பினரால் ஒரு நடவடிக்கை கொண்டு வரப்பட்டால், வாதியின் நற்பெயரைப் பாதிக்கும் அல்லது களங்கப்படுத்தும் ஒரு செயலாக இது இருக்கும்."

தற்போதைய வழக்கில் பிரதிவாதிகள் தங்கள் சட்டவிரோத

செயல்களை ஒப்புக்கொண்டனர், மேலும் தரப்பினர் வழக்கு நடவடிக்கைகளில் ஒரு சமரசத்தை பதிவு செய்வதன் மூலம் இந்த விவகாரத்தை தீர்த்தனர். சமரச விதிமுறைகளின்படி, பிரதிவாதிகள் வாதியின் வர்த்தக முத்திரை உரிமைகளை மீறியதற்காக இழப்பீடாக 1.6 மில்லியன் ரூபாவை வாதிக்கு வழங்க ஒப்புக்கொண்டனர். பிரதிவாதிகளின் வளாகத்தில் இருந்து கைப்பற்றப்பட்ட ஹார்ட் டிஸ்க்குகளை வன்

வட்டுகளின் உரிமையாளராக இருக்கும் வாதியிடம் ஒப்படைக்கவும் நீதிமன்றம் உத்தரவிட்டது. பிரதிவாதிகள் அவர்களின் ஊழியர்கள் மற்றும் முகவர்கள் வாதியிடமிருந்து தோன்றியதாகக் கூறப்படும் மோசடி மின்னஞ்சல்களை புழக்கத்தில் விடவோ அல்லது நாஸ்காம் என்ற வர்த்தகப் பெயரையோ அல்லது வாதியின் வேறு பெயர் / குறி மற்றும் முகவரியையோ பயன்படுத்துவதிலிருந்து தடுக்கப்பட்டனர் தங்கள் படத்தை களங்கப்படுத்தும் மேலும் அவர்களது இமேஜ் கெடுக்கிறது.

செயல்பாடு- 1

செய்தித்தாள் அறிக்கைகளைப் படித்து, மேலே விவாதிக்கப்பட்டபடி போலி அடையாளம், அவதூறு, ஏமாற்றுதல் போன்றவற்றைக் கையாளும் சில இணையவழிக் குற்றங்களை அடையாளம் காணவும். இத்தகைய செய்திகளைப் பின்தொடரவும், விளைவுகளை பகுப்பாய்வு செய்யவும்.

தன் மதிப்பீடு 3

குறிப்பு: உங்கள் பதில்களுக்கு கீழே உள்ள இடத்தைப் பயன்படுத்தவும்

உங்கள் பதில்களை இந்த பாடப் பகுதியின் இறுதியில் கொடுக்கப்பட்ட பதில்களுடன் சரிபார்த்துக் கொள்ளவும்.

1) '்பிஷிங்' என்ற சொல்லை விளக்குக.

.....

.....

.....

.....

.....

2) தரவு டிட்லிங் (Data Diddling) என்றால் என்ன?

.....

.....

.....

.....

11.6 பாட தொகுப்புரை

இந்த பாடப்பிரிவில் இணையவெளி கருத்து போன்ற இணையவழி சட்டம் தொடர்பான பல்வேறு அம்சங்களை நாம் விவாதித்தோம் - இணையவெளி ஒழுங்குமுறை தேவை; தகவல் தொழில்நுட்ப (ஐ.டி) சட்டத்தின் கீழ் இணைய குற்றங்கள் மற்றும் குற்றங்கள்; மற்றும் இந்தியாவில் இணையவெளியை ஒழுங்குபடுத்தும் சட்டம் ஆகியவை இதில் அடங்கும்.

இன்று இணையவெளி ஒரு புதிய தகவல்தொடர்பு ஊடகமாக உருவெடுத்துள்ளது, சமூக மற்றும் பொருளாதார நடவடிக்கைகளின் எண்ணிக்கை புதிய சவால்களுக்கும் புதிய வடிவங்களுக்கும் வழிவகுக்கும் ஒரு இடமாகும். இவற்றில் சில கணினிகள் மற்றும் நெட்வொர்க்குகள் சம்பந்தப்பட்டவை, அங்கு கணினி குற்றம் செய்வதற்கான ஒரு கருவியாகப் பயன்படுத்தப்படலாம் அல்லது கணினியே இலக்காக இருக்கலாம் அல்லது கணினி ஒரு குற்றத்திற்கு தற்செயலானதாகக் கருதப்படலாம். எனவே இணைய இடைத்தரகர்களின் பங்கு, இணைய பாதுகாப்பு, மின் நுகர்வோர் பாதுகாப்பு மற்றும் தனியுரிமை மற்றும் அறிவுசார் சொத்துரிமைகளைப் பாதுகாப்பதன் மூலம் தீங்கு விளைவிப்பதைத் தடுப்பதற்கான அவர்களின் தொழில்நுட்ப திறனை மறுக்க முடியாது. இடைத்தரகர்கள் தங்கள் கடமைகளைச் செய்யும்போது உரிய விடாமுயற்சியைக் கடைப்பிடிக்க வேண்டும் என்று விவாதிக்கப்பட்டது. மின்னணு பதிவுகள் மற்றும் தொழில்நுட்பம் சார்ந்த குற்றங்களை நிர்வகிப்பதற்கான பொருத்தமான சட்டம் தகவல் தொழில்நுட்ப சட்டம், 2000 ஆகும். கணினிகள் மற்றும் தொழில்நுட்பத்தின் பயன்பாடு அல்லது உதவியுடன் அல்லது அதன் மூலம் செய்யக்கூடிய பல பாரம்பரிய குற்றங்களையும் இந்திய தண்டனைச் சட்டம், 1860 இன் கீழ் கையாள முடியும் என்றும் விளக்கப்பட்டது.

11.7 தொடர்ந்து படித்தற்குரிய நூல்கள்

1. Dr.S.R. Myneni, Information Technology Law (Cyber Laws), Asia Law House, 2017
2. Gibson, William, Neuromancer, Harper Collins Publishers, London, 1995, p.67
3. Pavan Duggal, Cyber Law, Universal Law Publishing Co., Delhi, Second Edition, 2017
4. Prashant Mali, Cyber law & cyber crimes simplified, Cyber Infomedia, 4th edition. 2017
5. Vakul Sharma, Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce. Universal Law Publishing - An imprint of Lexis Nexis. 5th edition. 2016

11.8 தன் மதிப்பீடு விடைகள்

தன் மதிப்பீடு 1

1) இணையவெளி என்பது ஒரு பொருளின் இருப்பிடம் அல்ல, ஆனால் ஒரு மெய்நிகர் இடம். இணைய வெளியில் நுழைவதற்கு அணுகல் சாதனம் தேவை. அதாவது ஒருவருக்கு ஒருவித உடல் அணுகல் சாதனம் தேவைப்படுகிறது (கணினித் திரை, தொலைபேசி, முனையம், முதலியனவாக இருக்கலாம்) டிஜிட்டல் கம்ப்யூட்டிங் பவர் மற்றும் / அல்லது மென்பொருள் போன்ற ஒரு செயற்கை செயலாக்க பொறிமுறையுடன். இது இணைப்புகளின் நெட்வொர்க்கில் உள்ள பிற அணுகல் சாதனங்களுடன் இணைக்கப்பட வேண்டும். இது தனிநபர்கள் மற்றும் தனிநபர்களின் குழுக்கள் இடையே தொடர்பு மற்றும் தொடர்பு செயல்படுத்துகிறது அவர்களின் படைப்பு வெளியீடு, பெரும்பாலும் நேரம் மற்றும் வெளியிலிருந்து சுயாதீனமானது.

2) இன்று புதிய தகவல்தொடர்பு தொழில்நுட்பங்கள், மொபைல் போன்கள் மற்றும் பிற தகவல்தொடர்பு சாதனங்களின் பயன்பாடு ஆகியவை உலகளாவிய அளவில் அதிகார வரம்பு பற்றிய பாரம்பரிய கருத்துக்கு சவால் விடுகின்றன. இது ஒரு தனிநபரின் தனியுரிமை மீதான படையெடுப்புக்கு வழிவகுத்துள்ளது. இணையவெளி சமூக ஊடக குற்றங்கள், வதந்தி பரப்புதல், மின்னஞ்சல் ஸ்பூ஼பிங், ஸ்பேம்கள், சைபர் பின்தொடர்தல், அவதூறு மற்றும் பல்வேறு சைபர் கிரைம்களின் பிரச்சினைகளை சமாளிக்க பயனுள்ள சட்டம் நமக்குத்

தேவை, ஏனெனில் இந்த குற்றங்களின் தாக்கம் ஏற்படலாம் வழக்கமான குற்றங்களை விட அதிகமாக இருக்க வேண்டும். இந்த இணையவெளி குற்றங்கள் பொதுவாக போலி அடையாளத்தைப் பயன்படுத்தும் நபரால் செய்யப்படுகின்றன, இதனால் உடனடியாகவும் எளிதாகவும் அடையாளம் காண முடியாது.

தன் மதிப்பீடு 2

1) தகவல் தொழில்நுட்பச் சட்டத்தின் பிரிவு 2 (1) (w) மற்றொரு நபரின் சார்பாக ஸ்டோர்களைப் பெறும் அல்லது அந்த பதிவை அனுப்பும் அல்லது அந்த பதிவு தொடர்பான எந்தவொரு சேவையையும் வழங்கும் எந்தவொரு நபரையும் இடைத்தரகரை வரையறுக்கிறது. இடைத்தரகர்கள் பின்வருவனவற்றை உள்ளடக்குகின்றன: தொலைத்தொடர்பு சேவை வழங்குநர்கள்; நெட்வொர்க் சேவை வழங்குநர்கள்; இணைய சேவை வழங்குநர்கள்; வலை ஹோஸ்டிங் சேவை வழங்குநர்கள்; தேடுபொறிகள்; ஆன்லைன் கட்டண தளங்கள்; ஆன்லைன்-ஏல தளங்கள்; ஆன்லைன்-சந்தை இடங்கள் மற்றும் சைபர் க◌ஃபேக்கள்.

2) கட்டுப்பாட்டாளர் அல்லது தீர்ப்பளிக்கும் அலுவலரால் பிறப்பிக்கப்பட்ட உத்தரவினால் பாதிக்கப்பட்ட எவரும், மேற்சொன்னவற்றின் நகல் கிடைத்து நாற்பத்தைந்து நாட்களுக்குள், இந்த விஷயத்தில் அதிகார வரம்பைக் கொண்ட இணையவெளி மேல்முறையீட்டு தீர்ப்பாயத்திடம் மேல்முறையீடு செய்யலாம். உத்தரவு. எவ்வாறாயினும், இருதரப்பு ஒப்புதலுடன் ஒரு தீர்ப்பு அதிகாரியால் பிறப்பிக்கப்பட்ட உத்தரவிலிருந்து சைபர் மேல்முறையீட்டு தீர்ப்பாயத்திற்கு மேல்முறையீடு செய்யப்பட மாட்டாது.

தன் மதிப்பீடு 3

1) ◌ஃபிஷிங் என்பது உள்நுழைவு நற்சான்றுகள் மற்றும் கிரெடிட் கார்டு எண்கள் உள்ளிட்ட பயனர் தரவைத் திருட பெரும்பாலும் பயன்படுத்தப்படும் ஒரு வகையான சைபர் குற்றமாகும். பொதுவாக இது சில நம்பகமான நிறுவனத்தின் மாறுவேடத்தின் கீழ் ஒரு நபரால் செய்யப்படுகிறது.

2) தரவு டிட்லிங் என்பது ஒரு வகை சைபர் கிரைம் ஆகும், இதில் தரவு ஒரு கணினி அமைப்பில் உள்ளிடப்படும்போது, பெரும்பாலும் ஒரு தரவு நுழைவு எழுத்தர் அல்லது கணினி வைரஸால் தரவு மாற்றப்படுகிறது.