Data protection and Privacy Rights of Citizens: A significant Human Rights issue in India

Rakhi Sharma
Ph.D. Scholar, Faculty of Law, School of Law, Manipal University Jaipur

Dr. Maryam Ishrat Beg
Associate Professor, Faculty of Law, School of Law Manipal University Jaipur

Abstract: The growth of India's internet population and the speed at which the country is adapting to technology has made it a large market for many global players. New technologyis impacting India. The governmenthas recognized this, and created the "Digital India"initiative, which promises to have large disruptions in all sectors of society. In this digital ageof e-commerce, mobile apps, and banking etc., people also knowingly or unknowingly mayshare sensitive personal data. Users agree to provide personal data by checking the ‘I agree’box in their settings. They don’t need to read the privacy policy to do this and risk these sensitive details being leaked to hackers. In this paper we will take about the data protection and data privacy and reason why data leaks hampering of humanrights.

Keywords: Bitcoin,Cryptocurrency,Decentralizedcurrency,PayPal,DigitalCurrency.

I. INTRODUCTION

Users’ concern about their privacy on social media has spiked in recent years, largely due todatabreaches,whichledtoreconsideringtheirrelationshipswithsocialappsandtheinformation security in these apps. A specific incident is the story of Cambridge Analytica'sconsulting agency, which was dramatic and alarming. It is of high concern that Facebook hasbeen exploiting the private information of 50 million Americans during the 2016 election. Wemaynothavecontrolofourowndata, andthis is unjust.[1]

Social media users are increasingly worried about the businesses and also due to advertisersusingtheircontent.AnewstudybythePewTrusthasshownthat80%ofsocialmediausersareconcernedaboutthis.Asofnow,thereisnoregulationforlimitingexploitation.Organizationswhose job is to safeguard personal data are now under tighter scrutiny because of the rise inhigh profile cyber security breaches. Businesses and consumers need to protect sensitiveinformationinaworldthatisconstantlyconnected.

Cyber threats will also rise over the coming few years, so being prepared will act as the key.Privacy is important for most people who use the internet. There is no such thing as absoluteanonymity and this is especially true in the digital world because websites and social mediaplatformsfollowwhatpeopledoonline.Butyoucanprotectyourpersonaldatabydoingthingslikeusingprivate browsing extensionsandcreatingnewemailsfromtimetotime.[2]

It's becoming more and more difficult to secure your online presence. Scammers are trying toget the complete hold of your email address, also the social media trackers may collect yourdata,identitythievestrytostealit,andautomaticbotsaresharingitwithoutyouknowing.Dataandcybersecuritybestpracticesareimperativeintoday'ssociety.Itisjustasnecessarytosafeguardpersonaldataandeducateaudiencesonhowtheycanprotectthemselveswhenusingthe internet. Businesses are pouring a lot of money into advertising for their brands on socialmedia,andthat'swhymarketersneedaccuratedemographicstotargetthemwiththeirads.ToolslikeFacebookandInstagramletadvertisersmaximizetheaddollarstheyspend.Onedownsideto hyper-targeting customers is that they increasingly use ad blockers. For instance, customersare encouraged to use an ad blocker for the android or the similar sort of solution for the iOSdevices in order to get rid of the intrusive ads which are being popping up on each of thewebsite.[3]

Onlineadvertiserswillmanipulatesocialmediadatatofindcluesaboutyourinterestssothattheycanadvertisetoyou.

Someissueswhicharerelevanttodatasecurityanddataprivacy:

- **Data Scraping Challenges:** Data harvesters, who are usually research companies, trackpeople’s online activity and harvest personal data from the social media, also the job sitesandalsoonlineforums.Researchcompaniessellthisinformationtoothercompaniessothatthey can use it to make targeted ads for their products. It might be argued that peopleknowingly share this information on social media and thus it is free for anyone to use thedata. The issue with that is that researchers don't ask for the owner's consent beforehand,whichbringsupanethicsproblemaswellasaprivacyissue.
  “OnestrongargumentforseriousonlineprivacyviolationtakesplaceinMay2011.NielsenCo., a media-research company, was caught scraping every message off Patients [4] LikeMe'sonline forums, where

people talk about their emotional problems – in what they thinkisathesafe,alsotheprivateenvironment.”.

- **Facebook's newest security issue:** Facebook apps leak identifying information which isbeingcollectedbytheadvertisingandalsotheInternettrackingcompanies,withouttheusershaving any sort of clue. An app might request an “access token” during installation.However,ifyou havegrantedaccesstokensto certainapps,theymayshareyourdatawithadvertiserswithoutinformingyouoftherisks. SomeFacebookappslikeFarmvilleandGiftscanleakyouraccesstokenstotheadvertisers,asaresultgrantingthemthefullaccesstothepersonalprofiledatasuchasthechatlogs,thephotos, location and browsing history. There is no disclaimer whatsoever stating that theuser’sdatawillbetransferred. Thisputsonlineprivacyandalsosafetyatrisk.
  “There are apps that have been shown to leak information, examples of which includeFarmvilleandFamilyTree”.[5]
- **Onlinesocialtracking:**TheLike,Tweet etc.buttonsthatweusetosharecontentwithourfriends also serve as tracking tools for certain websites. These social website cookies areusedinbrowserswhenlogginginorcreatinganaccountandtheyhavetheabilitytoidentifyyou across different sites. This invasion into internet privacy can be seen when yourshoppingbehaviorsorinterests aretracked.
  “Otherwebsitesallowcompaniestoplacewithinads,cookiesandbeaconswhichcantrackyouandgatherinformationaboutwhatyouaredoingonapage.Thesetoolsaremainlyusedonline but mostly in websites dedicated to children, which raises a huge concern over thesafetyofchildren”.

II. DATAPROTECTION

The process of data protection is the safeguarding of the important collection data from thecorruptionandalso theloss,and providescapabilitiesforpurposeto restorethedata.TheDataprotectionwillalsoassurethatthedataisnotcorrupted,butinsteadisaccessibletoyouandonly youwhile abidingbyrelevantlaw.Itshouldbeavailablewhenneeded.[6]

The scope of data protection includes immutability, preservation, and deletion/destruction;which are all parts of ensuring data availability and usability. Traditional data protection alsoincludesthebackupandtherestorecopies,thepropersecuritymeasures,andprivacy(encryption). There are many ways to ensure that your data is constantly safe, such as securityproceduresandidentification.

Principleoftheprocessofdataprotection

- Data protection is crucial to ensure that data is always accessible and secure, followingvariouspoliciesandprocedures.
- Storagetechnologiescanprotectyourdatabymakinguseofdisk,tapes,orthecloudbackupinordertosafelystorecopies ofthedataandthenuse itincaseofdataloss.
- Additionaldataprotectionhasbeenintroducedintheformoftoolslikecloning,mirroring,replication, and snapshots. These data protection tools are better than traditional backupbecausetherecoveryprocessis near-instantaneous.[7]

LatestTrendsinDataProtection

Someofthelatesttrendsinthedataprotectionaredescribedbelow,

- **Hyper-Convergence:**Withhyper-convergedsystems,vendorsareintroducingstand-alonebackupandrecoverydevicesthatintegratecomputer,networkingandstorageinfrastructure.
  These new devices are replacing traditional data center gear, and are providing cloud-likecapabilities on-premises.
- **Ransom ware Protection:** There are many types of malwares, and ransomware encryptsthe dataonyourdevice.Traditionalbackupmethodsprotectfromthesetypesofencryptions. However, new models have the ability to overtake backup systems as well,making it moredifficult to restore old data. New backup solutions will not be affected bycyber-attacks. Byisolating the backups from the corporate network and encrypting data atrest,new backupsolutions canpreventransomwarefrominfectingbackups.[8]
- **Disaster Recovery as a Service:** “Disaster recovery as a service is a cloud-based solutionthatallowsanorganizationtocreatearemotecopyoftheirdataanduseittorestoreoperationsincaseofdisaster.InstantlyprovidemorereliabledatawithaDRaaSsolution.Theycontinuouslyreplicate datafromthe localdata centertoprovide alow recoverytimeobjective (RTO), meaning they can spring into action within minutes or seconds”.“InstantlyprovidemorereliabledatawithaDRaaSsolution.Theycontinuouslyreplicatedatafromthe localdatacentertoprovidealowrecovery

timeobjective(RTO),meaningtheycanspringintoactionwithinminutesorseconds".

- **Copy Data Management (CDM):** CDM solutions help companies streamline their dataprotection by reducing the number of backups they store. This reduces overhead andmaintenance, while also lowering storage costs. These solutions create automation andcentralizedmanagement,whichcutsprocessesdevelopmentdownandincreasesproductivity.[9]
- **Audit of Sensitive Data:** "Before adopting data protection controls, you must first audityourdatainfrastructure".Usethefollowing formulatoidentifywhatyourcompanyisusingand needs, and then create a plan for storage. "Data should be classified into sensitivitylevels, and should also be assessed to assess which data protection measures exist in theorganization, how effective they are, and what can be done to extend those measures. It iscrucial to know that often the biggest potential is in leveraging existing data protectionsystemsthatarelyingaroundorarenotusedconsistentlythroughouttheorganization".
- **AssessingInternalandExternalRisks:**Thesecurityteamshouldassesstherisksthatmayarise in their organization. This team should also design data protection programs aroundthese internal and external risks. Internal risks to IT security include issues with networkconfiguration, the use of a strong password, or username and password authentication. Agrowingthreatiscompromisedaccountsoremployeeswhohavebeenattackedbymalware."Externalrisksarisefromsocialengineeringstrategies,suchasphishing,malwaredistribution,andattacksoncorporateinfrastructure,likeSQLinjectionordistributeddenialofservice(DDoS)".

DataProtectionPolicy

Theorganizationhasidentifiedthemostrelevantthreats,andtheyhavecreatedadataprotectionpolicy to deal with them. Every data category has a different tolerance for risk, and protectionmeasures mustbe appliedaccordingly.[10]

Companies need to weigh the risks of data leakage with their data protection policies. Usehistoricalinformationtounderstandwhatapplicationsoraccountsneedaccesstosensitivedata.

- Security Strategy: The correct security strategy for data protection. Protect your sensitivedatafromthreatactors.Makesureyoudon'tunintentionallyreduceemployeeproductivity.Manycompaniesareintroducinga"bringyourowndevice"policythatiscausingemployeestohavetroubleaccessingdatafromthestoresorwheretheywork.
- ComplianceStrategy:Dataprotectionstrategiesneedtotakeintoaccountthattherearemanyregulationsaffectingtheirorganizationandthedifferentpartsofit.

RelatedResearchWorkinfieldofDataProtection

P. A. Indhumini Ranathunga and A. P. R. Wickramarachchi, 2022 report that data-driven businessesmustprotecttheirdatawithspecializedsolutionsasthevolumeandcomplexityincreaseproportionately." Astheuseofpersonaldataaffectsprivacyandsecurity, many countries have passed legislation to protect its citizens' information. GDPR isone of them,designedfor EU data processing companies. GDPR does not directly apply toSri Lanka butapplies to firms that deal with European Union counterparts — Sri Lankanfirms must complywith GDPR or risk being shut out of the European market. There has beenlittle research abouthow to best implement GDPR guidelines, but it was found that the currentresources availablefor Sri Lankan companies are not enough. To fix this problem, a new datagovernancemodel withmultiplestepswasdevelopedwhich wouldprovidesecuredatahandling".Thisstudyallowscompaniestocreateadatagovernancemodelthatensurestheyarecompliantwith GDPRprinciples.[11]

M.Joshi,etal.2021highlightedthatifacompanyisgoingtouseanoutsideservicetostoretheir data, they must think about their security. The company should understand their securitychallengesbeforeoutsourcingthedatainthecloudsothattherearenorepercussionslateron.[12]**Dr.Chhatwal, 2020**discussedhowprotectingprivilegedcommunicationsisofhighimportanceforthelegalteams,suchastheattorney-clientletters,litigationstrategiesandotherinformationthat should not be disclosed. To protect against leaks and breaches, information is oftenreviewedbeforeit'sdisclosedtomakesureitcan'tbeusedagainstthem.Thisreviewprocessistypically time-consuming and expensive. To reduce the number of documents that need to bereviewed for privileged information, data about client and outside counsel workflows wascollected and put into an algorithm that assessed the probability of privileged information as adocumentisread.Keywordsearchesareapopularwayoftargetingprivilegedinformation.Thissearchreliesonkeywordsandisofteneffectivebutatthesametimeitcanalsoreturnirrelevantpages,whereyou'reunlikelytofindprivilegedinformation. Machinelearningisbeingusedinlegal teams to target privileged information as keywords are not always providing outcomes.Keyword searching has many disadvantages, so this alternative can provide the policies theyneed while excluding unneeded ones. The authors use machine learning and convolutionalneuralnetworkstoidentifyprivilegeddocuments.TheirapproachcombineskeywordsearchingwithCNN.[13]

III. DATAPRIVACY

"Data privacy is the ability for a person to determine how their personal data is shared.Besideswantingtoexcludepeoplefromaconversation,manypeoplewanttocontrolorpreventcertaintypesof personaldatacollection".

"As Internet usage has increased over the years, so has the importance of data privacy.Websites, applications, and social media platforms often need to collect and store personaldata". Data protection laws aim to protect your right to privacy in many jurisdictions. Peoplearemorewillingtoengagewithorganizationswhentheyproducequalitycontent andcareabouttheirpersonaldata.[14]

Personal data can be used if the owner of the data doesn't want that to happen, if it is alsokept safe,orifthepeoplecanthencontrolhowtheirinformationisthen beingused.Criminalsalsocanuse metadatatoaidinidentitytheftorannoyusers.

Entitiesmaysellinformationabouttheuserwithouttheirconsent,whichcanthenresultsintheunwantedmarketingorsortsofadvertising.Theabilitytoexpressoneselfisrestrictedwhenpeople'sactionsarebeingmonitored,specificallyin repressivegovernments.Therepercussionsof unfair data gathering can be completely detrimental. They can harm individuals, as well asbusinesseswithlegalconsequencesandfines.[15]

Aperson'srighttoprivacyisimportant,andmanypeoplebelieveitshouldbeahumanright.It'snotjusthowotherpeopleinfringeonyourprivacythatmatters,butyourownright.Websitesoftentrackuserbehaviorandstorescookiestostoreyouractivities.Whilemostcountriesrequirewebsitecreatorstowarnusers,thereisstillalevelofuncertaintyinvolved. Individualsmayalsonot be aware of the point that how their data is then being used on other online services, andtheymaynotalsohavecontroloverthefactthat,whathappenstotheirownpersonaldata.

Often, the terms and conditions for accessing applications are hard to understand. Theseterms may require users to share sensitive information. The next generation of social mediaplatformsismaking iteasierthaneverinordertofindsomeoneonline.Also,Socialmediapostsoftencontainmorepersonalinformationthan peoplethinkabout,andwiththat,socialnetworksarecollectingmoredata.[16]

Cyber attackers try to steal user data to use on their computer, which can be used in manypurposes.Forexample,theymaytrickusersintorevealingpersonalinformationorcompromisethecompany's computerwithpersonaldata.DataPrivacyProtectionLaws

Dataprivacylawsalsovaryfromonecountrytoanothercountry,dependingonthetypeofdatatheystore.However,hereare some ofthemostcommondata privacylaws:

- **CaliforniaConsumerPrivacyAct(CCPA):**Youhavetherighttoknowhowyourdataisbeing handled and who has it, and you can remove it from the system. A new privacy actwascreated:"CaliforniaConsumerPrivacyAct(CCPA)whichwentintoeffect onJanuary1, 2020".
- **HealthInsurancePortabilityandAccountabilityAct(HIPAA):"**TheHealthInsurancePortabilityand AccountabilityActisalawthat definesthewayorganizationsshouldstore,share, and secure patient information". HIPAA regulations specifically affect healthcareprovidersandhospitals,butevenbusinessesinsimilarindustrieswithlesspatientinformationmustapplythesetoprotectsecurity.[17]
- **Children'sOnlinePrivacyProtectionAct(COPPA):**COPPAisa2000lawthatdefinesbusinesses'rightstocollectandshareinformationaboutchildren.Ifyouhandledataforkidsundertheageof12,thenyoumustprotecttheir screennamesand emailaddresses.
- **PCI-DSS:** PCI-DSS focuses on stopping card fraud and identity theft. It is a compliancestandardforstoringcustomerdata.PCI-DSS,aregulationtostoreconsumer financialdata,mustbe followedby any organization.Theseinclude online storesas well as smallorganizations.
- **The Cookie Law:** Cookies store website information on your device to save you time andmakeyoure-enterlessinformationinthefuture.Cookiesmayalsosendinformationinthefutureordiscloseitifthedeviceisstolen.Websitesneedtogetuserconsentbeforetheycanstoreacookieonauser'sdevice.
- **GeneralDataProtectionRegulation(GDPR):**GDPRisalawthatassurestheprivacyofEuropean resident data. Violating GDPR could result in a hefty fine and penalties. UnderGDPR,organizationsstoringconsumerdatafromtheEUarerequiredbylawtoofferawayto have user data removed from their system, and to specify how they are storing, sharing,andcollectingthatdata.[18]

Research'shighlightedNeedofDataPrivacy

Cybersecurityisalarge,successfulindustrythat employsmanypeople.In2021,PolonetskyandSparapanipredictedthiswouldonlygrowinnumbers.Experiencedcy bersecurityprofessionals know what they need to do, while privacy technology is still maturing. Privacytechnology is well developed, but continuing to evolve rapidly. Many companies such asGoogle, Apple, LinkedIn and Amazon have had success in addressing privacy concerns. Thisarticle reviews the findings of a report on how privacy technology companies are maturing. Itciteshowtheindustryisdevelopingandwhatfeaturesarebeingofferedbythetopcompanies.[19]

T.S.ReshmiandS.DanielMadanRaja,2019notifiedthatsocialnetworkplayamajorrolein how we live. Facebook, the most popular social network, currently has 2.23 billion usersworldwide.Peopleareawareofthesecurityrisksandtheyrelyontheprivacysettingsavailableonsocialnetworks toprotecttheirdata.Dataonsocialnetworksisn'tactuallydeleted.Thedata'sstillthere,anddeleting it won't makeanydifference.Youcouldjust deletesomepersonalinfo,but that wouldn't necessarily keep it from being retrieved. Methods for deleting data must bedeveloped,andthispapertalksabouttherisksofdeletingdatainthisWeb-basedworld.[20]

J. Nicholson and I. Tasker, 2017 specified that the education market in the UK is using scopesharing. However, this approach leaves gaps and is incompatible with GDPR. Data Exchangeis an ethical data integration platform that uses standards similar to “The Family EducationalRights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act(HIPAA)”. Data Exchange has a proof-of-concept solution to the third party data problem byupdatingpermissions.[21]

IV. DATAPROTECTIONANDDATAPRIVACY:HUMANRIGHTSISSUE

TheGovernmentofIndiablockedover100mobileappsinSeptember2020toprotectthepublicbecause they were a security risk. The Indian government has issued a warning about thesesecurity hazards. MEITY (Ministry of Electronics and Information Technology) also receivedcomplaints about misuse of mobile apps. To safeguard the interests of Indian cyberspace,MEITY took this drastic measure. They collected, mined and profiled data to determine anypossiblethreats.Thiswillhelpmaintainthesovereigntyandintegrityof India'scyberspace.[22]

WiththeMEITYdecision,it isclearthatIndianeedsstrongdataprotectionlaws.Accordingto Statistic, India is the second largest online market worldwide. There are over 974 millionusers in 2025.

“The right to privacy is an integral part of our constitution and was affirmed by the nine-judgebenchoftheSupremeCourtin2017.Article21oftheConstitutionofIndiastatesthatNopersonshallbedeprivedofhislifeorpersonallibertyexceptaccordingtoprocedureestablishedbylaw.Thisstatement,calledtheRighttoPrivacy, wasaffirmedin24thAugust2017byanine-judgebench,whodeclaredtherighttoprivacyasanintegralpartofPartIIIoftheConstitution,alsoknownas FundamentalRights”.

Abenchofninejudgeswerebroughttodecideifprivacyisafundamentalright.“In2017,abenchoffivejudgesinthe SupremeCourt washearingthecaseaboutAadhaarandtherighttoprivacy.Theysaidthattheyneededanine-judgebenchtofirstdecideifprivacyisafundamentalright, before deciding on the main Aadhaar case. The Attorney General argued that the nine-judgebenchwasnecessarytodecidewhetherprivacyisafundamentalright.TheSupremeCourthasrefusedtotakethisintoconsiderationinmanypastcases,meaningit needstobethoroughlyexamined”.[23]

Indiaislackingalawfor individualdata.Dataprotectionprotectionsonethatareavailable,however, they are also contained in the mix of statutes, the rules and also the guidelines. Indiaislackingalawforindividualdata.

SPDI Rules are India's primary law for cybercrime. SPDI Rules do not cover informationcommunicated through non-electronic methods. The IT Act, 2000 came into force in Octoberof 2000 and there were no provisions for the protection of sensitive personal informationprovidedinelectronicform.AnActwasneededtoprovidetheseprovisions.

The Information Technology Act, 2008 came into force on October 27, 2009. Section 43Aof the Act said IF (in accordance with any agreement entered into by him with a computerresourceprovider):

If a corporation is negligentin protecting sensitive data and then as a result of theirnegligence,theperson'sdataisstolenorisrecreatedwithnegativeconsequences,thecorporationcanbeliablefor damages.

Also,Section72A,accordingtowhich:

Ifsomeonebreaksacontracttodiscloseinformation,theymayfacethreeyearsinjailanduptofivelakhrupeesin fines.IfyouviolatetheITAct,youmayhave topayafineofuptoINR10,000.“TheactspecificallystatesthatanypersonviolatinganyprovisionsofthisActorofanyrules or regulations made thereunder shall be punishable with imprisonment for a term whichmayextendtooneyearandshallalsobeliabletosuchfine(aminimumofRs.500forviolationnotinvolvinglossofinformationorwhoselosshasbeenremediedin72hours),andinthecaseofsecondorsubsequentconvictionwithimprisonmentwhichmayextendtotwoyearsandshallalsobeliabletosuchfine(Rs. 5,000).”

If a member of the IT Act violates your personal database, they will be sentenced to twoyears inprisonorfined1,00,000rupees.[24]

This Act will also apply if the crime hacker has ever touched a computer or network in India.The Indian Information Technology Act and Rules apply only to 'sensitive personal data andinformation' collected through 'computer resources', as opposed to the Indian Personal DataProtectionAct,whichappliestoallpersonaldatainIndia.

Digital currencies offer the ability to transcend international borders, which would help fostereconomicgrowthandreliability.Itwouldalsobeinexpensive,easy,andfast.Digitalcurrenciesareabletohelpboostthetradeofthecountry,whileincreasingitsfinancialhealth.Withtheriseofdebitcardsandelectronictransfers,thesystemischanging.Governments,banks,businesses, andpeoplenolongerusephysicalmoneytotransferfunds.Theyinputnumbersintoelectronicledgersandhavethirdpartieschangethenumbers.Withthegrowingpopularityofcryptocurrencies, some are fearful over potential changes. Cryptocurrencies have had billion-dollarimpactthathas yettobeseen.[25]

V. CONCLUSION

“In the digital age, we typically apply the concept of data protection to our critical personalinformation. This can include things like social security numbers, health and medical records,financialdata,bankaccount andcreditcardnumbers,andevenbasicbutsensitiveinformationincluding full names, addresses and birthdates”. To ensure that data is safe and secure, it isimportant to have access controls in place. Personal information should not have uncontrolledaccess to individuals who could be at risk of fraud or identity theft. Data breaches are a bigproblembecausetheymake data like trade secrets public. And if a competitorgetsholdofthatinformation,they'llhaveanedgeonyou.Dataprotectionlawsprotectonlineinformation,asitiswheremost ofourliveshappen.Cybersecurityconcernsaregrowingbecauseoftheneedforcontinual protection of the data that we store online. Data protection laws are necessary forIndia, as it is one of the only countries in the world without a comprehensive and modern dataprotection law. Data protection laws work best when they work together with internationalcounterparts.

REFERENCES:

1. “Social media privacy issues for 2020: Threats & risks. (n.d.). Tulane.edu. Retrieved from https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020”
2. “Social media privacy issues for 2020: Threats & risks. (n.d.). Tulane.edu. Retrieved from https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020”
3. “Social media privacy issues for 2020: Threats & risks. (n.d.). Tulane.edu. Retrieved from https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020”
4. “Privacy violations – the dark side of social media... - BullGuard. (n.d.). Bullguard.com.
5. “Privacy violations – the dark side of social media... - BullGuard. (n.d.). Bullguard.com.
6. “What is data protection? (2021). Snia.org. Retrieved from https://www.snia.org/education/what-is-data- protection”
7. “What is data protection? (2021). Snia.org. Retrieved from https://www.snia.org/education/what-is-data- protection”
8. “Nakar, O., Lynch, B., & Lee, G. (n.d.-b). Data protection. Learning Center. Retrieved from https://www.imperva.com/learn/data-security/data-protection/”
9. “Nakar, O., Lynch, B., & Lee, G. (n.d.-b). Data protection. Learning Center. Retrievednhttps://www.imperva.com/learn/data-security/data-protection/”
10. “Nakar, O., Lynch, B., & Lee, G. (n.d.-b). Data protection. Learning Center. Retrieved https://www.imperva.com/learn/data-security/data-protection/
11. “P. A. Indhumini Ranathunga and A. P. R. Wickramarachchi, General Data Protection Regulation(GDPR) Adoption in Sri Lankan Businesses: A Data Governance Model, 2022 2nd International Conference on Advanced Research in Computing (ICARC), Belihuloya, Sri Lanka, 2022, pp. 266-271”.
12. “M. Joshi, S. Budhani, N. Tewari and S. Prakash, Analytical Review of Data Security in Cloud Computing, 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, United
13. “Dr. Chhatwal, R. Keeling, P. Gronvall, N. Huber-Fliflet, J. Zhang and H. Zhao, CNN Application in Detection of Privileged Documents in Legal Document Review, 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 2020, pp. 1485-1492”.
14. “Privacy violations – the dark side of social media. BullGuard. (n.d.). Bullguard.com. Retrieved from https://www.bullguard.com/bullguard-security-center/internet-security/social-media-dangers/privacy-violations-
15. “Social media privacy issues for 2020: Threats & risks. (n.d.). Tulane.edu. Retrieved from https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020”
16. “Social media privacy issues for 2020:Threats & risks.(n.d.).Tulane.edu.Retrieved from

https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020"

17. What is data privacy? (2021, June 29). Proofpoint. https://www.proofpoint.com/us/threat-reference/data- privacy
18. What is data privacy? (2021, June 29). Proofpoint. https://www.proofpoint.com/us/threat-reference/data- privacy
19. "J. Polonetsky and T. Sparapani, A Review of the Privacy-Enhancing Technologies Software Market, in IEEE Security & Privacy, vol. 19, no. 6, pp. 119-122, Nov.-Dec. 2021."
20. "T. S. Reshmi and S. Daniel Madan Raja, A Review on Self Destructing Data:Solution for Privacy Risks in OSNs, 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 2019, pp. 231-235"
21. "J. Nicholson and I. Tasker, DataExchange: Privacy by design for data sharing in education, 2017 International Conference on the Frontiers and Advances in Data Science (FADS), Xi'an, China, 2017, pp. 92-97".
22. "Personal data protection law in India., Legal500.com. Retrieved from https://www.legal500.com/developments/thought-leadership/personal-data-protection-law-in-india/"