International Research Journal Multidiciplinary Sciences ISSN: Awaited
Vol 1 Issue 3 March 2025 PP 35-42

DATA SECURITY AND PRIVACY

[1]VaibhavSingh, [2]Bhawna Kaushik, [3]Priya Gupta , [4]Anam Shariq
1.niu-23-11977@niu.edu.in
2. bhawna.kaushik@niu.edu.in
3. priya.gupta@niu.edu.in
[1,2,3]NoidaInternationalUniversity,Sector17A,GreaterNoida, [4]Birla Public School Qatar

ABSTRACT

As people, organizations, and governments depend more and more on digitalplatforms for communication, transactions, and information storage in the current digitalera, data privacy andsecurityhaveemergedascriticalissues.Theamountofsensitiveand personaldatabeing gathered, processed, and shared has increased dramatically due to the quick development of technology, increasing its susceptibility to misuse, illegal access, and cyberattacks. Various legal frameworks, such the California Consumer PrivacyAct (CCPA) and the GeneralData Protection Regulation (GDPR), have been created to address these dangers by establishing criteria for company responsibility, user rights, and data protection. However, jurisdictional disparities, changing cyberthreats, and the complexity of new technologies like cloud
computing,blockchain,andartificialintelligencemakeitdifficult toenforcetheselaws.

INTRODUCTION

The right to privacy and the concomitant requirement to protect personal information has garneredsignificant attentionwiththedawnoftheinformationage.Whilethe internet and online information-sharing and data collection increase at an exponential rate, legislative developments have failed to keep pace and adequately protect personal information.
However, with time,African states and regional and continentalbodies have begun to adopt dataprotection-relatedinstrumentsandregulations inanattempttoremedyandvindicatethe privacyrights of their citizens. This module focuses on data protection inAfrica and the related concepts of the ‘right to be forgotten’, encryption and surveillance.

THE RIGHT TO PRIVACY

There is an increasing recognition that the right to privacyplays a vitalrole in and of itself and in facilitating the right to freedom of expression. For instance, reliance on the right to privacyallows individualstoshareviewsanonymouslyincircumstanceswheretheymayfear being censured for those views, it allows whistle-blowers to make protected disclosures, and it enables members of the media and activists to communicate securely beyond the reach of
Unlawful government interception.

KEY PRINCIPLES OF DATA PRIVACY

Most data protection laws are built on a set ofkey principles, which establish the foundation for everything relatedto dataprivacyandtheprotectionofpersonaldata.Therearesevenkey data privacy principles that form the fundamental conditions that organisations must follow when processing personal data. Processing personal data in line with these key principles is essential for good data protection.

The Principles are -

Lawfulness, fairnessandtransparency:Youshouldalwaysprocesspersonaldatainafair,lawful and transparent manner.

Purposelimitation:Youshouldonlyprocesspersonaldataforaspecifiedandlawfulpurpose.

Dataminimisation:Youshouldensurepersonaldataiskeptuptodate,andthatnecessarymeasures are in place for correcting and updating inaccurate data.

Accuracy:You mustnotkeeppersonaldataforlongerthanyouneed it.

Storagelimitation:Youmustnotkeeppersonaldataforlongerthanyou needit.

Integrityandconfidentiality: You mustimplementadequatesecuritycontrolstoensurethat personal data is protected against loss, destruction or damage.

Accountability:You must haveappropriatemeasuresandrecordsinplacetobeabletodemonstrate your compliance.

CONCEPT OF PRIVACY ININFORMATION SECURITY

Personalinformationisanyinformationrelatingtoanidentifiableindividual56oran identified or identifiable natural person.57 It includes information such as an individual's name, phone number, address, e-mail address, licence number of an automobile, physical characteristics (facial dimensions, fingerprints, handwriting, etc.), credit card number and familyrelationship. In appropriate access to and collection, analysis and use of anindividual's personal information have an effect on the behaviour of others towards that individual, and ultimately have a negative impact on his/her social standing, property and safety. Therefore,

personal in formation should be protected from improper access, collection,storage,analysis and use. In this sense, personal information is the subject of protection.

The passive concept of privacy includes the right to be let alone and the natural right related to the dignityof human beings. It is connected to the law prohibiting trespass. The active concept of privacy includes self-control of personal information or the right to
manage/control personal information positively, including the right to make corrections to effects resulting from incorrect personal information.

PRIVACY IMPACT ASSESSMENT(PIA)

APrivacy ImpactAssessment (PIA) is a systematic process of investigating, analysing andevaluatingtheeffect on thecustomers'orthenation'sprivacyoftheintroduction of new information systems orthe modification of existing information systems. PIAis based on the principle of preliminary prevention—i.e. prevention is betterthan cure. It is not simply a system evaluation but the consideration of the serious effects on privacy ofintroducingorchangingnewsystems.Thus,itisdifferentfromtheprivacyprotection audit that ensures the observance of internal policy and external requirements for privacy. Because a PIAis conducted to analyse the privacy invasion factorwhen a new system is built, it should be performed at the early phase of development, when adjustments to development specifications are still possible. However, when a serious invasion risk occurs in collecting, using and managing personal information while operating the existing service, it would be desirable to perform a PIAand then modify the system accordingly.

- PIAgenerallyconsistsof3 Steps:

- ConceptualAnalysis
- DataFlowAnalysis
- FollowUpAnalysis

SECURITY & PRIVACY IN CONTEXT OF CLOUD

The adoption of public cloud services , a large part of yournetwork , system, applications, anddatawillmove underthird-party providercontrol.The cloud services delivery model will create islands (clouds) of virtual perimeters as well as a security modelwith responsibilitiesshared between thecustomerand thecloud serviceprovider (CSP).Thissharedresponsibilitymodelwillbringnewsecuritymanagementchallenges to the organization's IT operations staff. With that in mind, the first question a chief information security officer (CISO) must answer is whether she has adequate transparency from cloud services to manage the governance (shared responsibilities)

and implementation of security management processes (preventive and detective controls)toassurethebusinessthatthedataintheclouldisappropriatelyprotected.The answerto this question hastwo parts: whatsecurity controlsmust the customerprovide overand above the controls inherent in the cloud platform, and how must an enterprise's security management tools and processes adapt to manage security in the cloud. Both answersmust be continually reevaluated based on the sensitivityofthe data and the service-level changes overtime.As a customerof the cloud, you should start with the exercise ofunderstanding the trust boundary ofyourservicesin thecloud.You should understand allthe layersyou own, touch, orinterface with inthecloud service— network, host, application, database, storage, and web services including identity services(seeFigure6-1).YoualsoneedtounderstandthescopeofITsystem managementandmonitoringresponsibilitiesthatfallonyourshoulders,including access, change,

configuration, patch, and vulnerability management.

MatureITorganizationsareknowntoemploysecuritymanagementframeworks,such as ISO/ IEC 27000 and the Information Technology Infrastructure Library (ITIL) service management framework. These industry standard management frameworks provideguidanceforplanningandimplementingagovernanceprogramwithsustaining management processes that protect information assets. Forexample, ITILgives a detailed description of a number of important IT practices with comprehensive checklists,tasks,andproceduresthatcanbetailoredtoanyITorganization.Akeytenet of ITIL, and one that is applicable to cloud computing, is that organizations (people, processes) and information systems are constantly changing. Hence, management frameworks such as ITILwill help with the continuous service improvement that is necessary to align and realign IT services to changing business needs. Continuous service improvement means identifying and implementing improvements to the IT servicesthatsupportbusinessprocessessuchas salesforceautomationusingacloud serviceprovider. Giventhedynamiccharacteristicsofcloudcomputingservices, the activitiespresentwithinthesecuritymanagementprocessesmustbecontinuallyrevised to remain current and effective.

In short, security management is a constant process and will be very relevant to cloud securitymanagement.ThegoaloftheITILSecurityManagementframeworkisdivided into two parts:

- Realizationofsecurity requirements

Security requirements are usually defined in the SLAas well as in otherexternal requirements,whicharespecifiedinunderpinningcontracts,legislation,andinternally or externally imposed policies.

- Realization ofabasiclevelofsecurity

Thisisnecessarytoguaranteethesecurityandcontinuityoftheorganization andto reach simplified service-level management for information security management.

SECUIRTY IN ARTIFICIAL INTELLIGENCE(AI):

AI-based solutions permeate the way we live and do business, questions on ethics, privacy and security will also emerge. Most discussions on ethicalconsiderations ofAI areaderivationoftheFATframework(Fairness,AccountabilityandTransparency).A consortiumofEthicsCouncilsateachCentreofResearchExcellencecanbesetupand it would be expected that all COREs adhere to standard practice while developingAI technology and products.

Data is one of the primary drivers ofAI solutions, and thus appropriate handling of data, ensuring privacy and security is of prime importance. Challenges include data usage without consent, risk of identification of individuals through data, data selection biasandtheresultingdiscriminationofAImodels,andasymmetryindataaggregation. The paper suggests establishing data protection frameworks and sectorial regulatory frameworks, and promotion of adoption

of international standards.

The large amount of data they can create, smart cities are especially amenable to application ofAI, which can make sense of the data being generated, and transform it intopredictiveintelligence– thustransitioningfromasmartcitytoan 'intelligentcity'. However, thewiderangeofconnecteddevicesalso givesriseto increased risksin cyber security, with harmful actors such as hackers now capable of affecting city scale infrastructure.

INTELLLIGENT SAFETY SYSTEMS

AItechnologycouldprovidesafetythroughsmartcommandcentreswithsophisticated surveillance systems that could keep checks on people's movement, potential crime incidents, andgeneralsecurityofthe residents.Socialmediaintelligenceplatformscan provideaidtopublicsafetybygatheringinformationfromsocialmediaandpredicting potential activities that could disrupt public peace. In the city of Surat, the crime rate has declined by 27% after the implementation ofAI powered safety systems.

CISControlsforconsideration:InContextOfSecurity

Bearinginmindthebreadthofactivityfoundwithinthispatternandhow actors leverageawidecollectionoftechniquesandtactics,therearealotofsafeguardsthat organizationsshould considerimplementing.Asmallsubset—including the CIS Control Number—isbelow,whichshouldserveasastartingpointforbuildingoutyourownrisk assessments to determine what controls are appropriate to your organization's risk profile.

ProtectingDevices

- EstablishandMaintainaSecureConfigurationProcess

- EstablishandMaintainaSecureConfigurationProcessforNetwork Infrastructure
- ImplementandManageaFirewallonServers
- ImplementandManageaFirewallonEnd-UserDevices Email and Web

Browser Protection

- UseDNSFilteringServices Malware

Defenses

- DeployandMaintainAnti-MalwareSoftware
- ConfigureAutomaticAnti-MalwareSignatureUpdates Continuous

Vulnerability Management

- EstablishandMaintainaVulnerabilityManagementProcess
- EstablishandMaintainaRemediationProcess Data Recovery
- EstablishandMaintainaDataRecovery Process
- PerformAutomatedBackups
- ProtectRecoveryData
- EstablishandMaintainanIsolatedInstanceofRecoveryData ProtectingAccounts
- EstablishandMaintainanInventoryofAccounts
- DisableDormantAccounts Access

Control Management

- EstablishanAccessGranting/RevokingProtocol
- RequireMFAforExternally-ExposedApplications
- RequireMFAforRemoteNetworkAccess Security

Awareness Programs

- SecurityAwarenessandSkillsTraining

KeyPoints:DataPrivacy,Ethics,andProtection

1. GeneralPrinciples

1. Dataprivacyisafundamentalhumanright,recognizedunderinternational conventions.
2. Theuseofbigdatamustalignwithhumanrightsprinciplesandethical considerations.
3. Datashouldonlybeaccessed,analyzed,orused forlawful,legitimate,andfair purposes.
4. TheUNDGemphasizesaharmonizedframeworkforresponsibledata practices.
5. Privacyrisksshouldbeproactivelymanagedwithsecurityandethical safeguards.

2. Lawful,Legitimate,andFairUse

6. Datamustbecollectedandprocessedincompliancewithnationaland international laws.
7. Consentshouldbefreelygiven,explicit,informed,anddocumented.
8. Datashouldnotbeusedinwaysthat causeharmorviolatehumanrights.
9. Theremustbeaclearpurposefordatacollection,withlimitationson repurposing.
10. Organizationsshouldavoidunjustifiedoradverseeffectsonindividualsor groups.

3. RiskMitigationandEthicalConsiderations

11. Dataprivacyconcernsshouldbeaddressedbeforestartingdataprocessing.

12. Organizationsshouldconductrisk-benefitassessmentsbeforeusingbigdata.

13. Sensitivedatamustbehandledwithstrictersecurity measures.

14. Ethicsshouldbeincorporatedintodataprocessingdecisions.

15. Riskassessmentsshouldincludephysical,emotional,andeconomicharms.

4. SensitiveDataandContextAwareness

16. Stricterprotectionsapplytovulnerablegroups(children,refugees,at-risk populations).

17. Contextcan turn non-sensitivedataintosensitivedata(e.g.,politicalsituations).

18. Dataonreligiousbeliefs,health,ethnicity,orfinancialstatusrequiresextra security.

19. Bigdataanalyticsshouldnotdiscriminateorcauseunintendedbias.

20. Consultationwithaffectedgroupsisrecommendedwhenprocessingsensitive data.

5. DataSecurityMeasures

21. Datasecurityisessentialtoprotectprivacyandprevent breaches.

22. Encryptionshouldbeappliedtoallstoredandtransmittedsensitivedata.

23. Firewallsandaccesscontrolsshouldlimitunauthorizeddataaccess.

24. Organizations should implement monitoring mechanisms fordata usage.

25. The principle of"PrivacybyDesign"should be embedded in all processes

CONCLUSION

Aspeople,companies,andgovernmentsdependmoreandmoreontechnologyinthe digitalage, datasecurityandprivacyhaveemergedaskeyissues. Significant regulatory concernsaswellaspreviouslyunheard-ofopportunitieshavebeenbroughtaboutbythe quick development of big data, artificial intelligence, and cloud computing. Because ensuring data privacy necessitates striking a delicate balance between innovation and protecting individual rights, numerous legislative frameworks, including the CCPA,
GDPR,and other international data protection regulations, have been developed.

Nevertheless,issues with enforcement,international data transfers,business responsibility, and government monitoring still exist in spite of these legislative actions. Establishing a single international standard for data security is challenging due to the fragmented nature of rules across everaljurisdictions,which makes compliance efforts more challenging. Furthermore, new technologies likeAI-driven analytics, biometrics, and the Internet of Things (IOT).

References

CaliforniaLegislativeInformation.(n.d.).*CaliforniaConsumerPrivacyAct(CCPA).*

EuropeanUnion.(2016).*GeneralDataProtectionRegulation(GDPR).*

HarvardLawReview.(n.d.).*Privacyanddataprotectioninthedigitalage.*

InternationalTelecommunicationUnion.(n.d.).*GlobalCybersecurityIndex.*

MassachusettsInstituteofTechnology.(n.d.).*AI,bigdata,andprivacyconcerns.*MIT Technology Review.

NationalInstituteofStandardsandTechnology.(n.d.).*NISTPrivacyFramework.*

StanfordInternetObservatory.(n.d.).*Thechallengesofdigitalprivacy.*

UnitedNationsDevelopmentGroup.(n.d.).*Dataprivacy,ethics,andprotection:Guidance note on big data for achievement of the 2030 agenda.*

World Economic Forum. (n.d.). *The global risks report.*

MediaDefence.(2020).*Dataprivacyanddataprotection.* Data Governance. (n.d.).

Privacy and security quotes.

PricewaterhouseCoopers.(n.d.).*DataprivacyinEgypt:Whatyouneedtoknow.*

UnitedNationsAsianandPacificTrainingCentreforICT.(2021).*Informationsecurityand privacy module.*

UniversityofScienceandTechnology.(2018).*Securityandprivacymodule.*

NITIAayog.(2023).*Nationalstrategyforartificialintelligence.*

UnitedNationsSustainableDevelopmentGroup.(n.d.).*Bigdataforsustainable development.*