Probeklausur

Informatik und Gesellschaft

Universität:	Technische Universität Berlin
Kurs/Modul:	Informatik und Gesellschaft
Bearbeitungszeit:	120 Minuten
Erstellungsdatum:	September 19, 2025

Zielorientierte Lerninhalte, kostenlos!
Entdecke zugeschnittene Materialien für deine Kurse:

https://study.AllWeCanLearn.com

Informatik und Gesellschaft

Aufgabe 1.

(a) Beschreiben Sie den Begriff *Soziotechnisches System* und nennen Sie zwei konkrete Beispiele aus dem Kontext von Informatiksystemen in Organisationen.

(b) Diskutieren Sie ein Spannungsfeld zwischen Datenschutz und Transparenz in einer öffentlichen Verwaltung und skizzieren Sie zwei daraus resultierende Folgeentscheidungen.

(c) Analysieren Sie das folgende Fallbeispiel-Szenario: Eine mobile Anwendung sammelt Standortdaten ihrer Nutzerinnen und Nutzer, um personalisierte Dienste anzubieten. Identifizieren Sie mögliche ethische Dilemmata und benennen Sie Kriterien, anhand derer Konflikte abgewogen werden könnten.

(d) Ziehen Sie eine kurze Schlussfolgerung zu den Auswirkungen dieser Spannungsfelder auf die Gestaltung von IT-Systemen in der Gesellschaft.

Aufgabe 2.

(a) Beschreiben Sie die Grundprinzipien der Datenschutz-Grundverordnung (DSGVO) im Kontext eines Unternehmens, das digitale Dienste anbietet. Nennen Sie drei zentrale Rechte betroffener Personen und drei Pflichten von Verantwortlichen.

(b) Nennen Sie drei regulatorische Regime, die auf IT-Systeme in Deutschland Einfluss haben, und erläutern Sie jeweils eine zentrale Auswirkung auf die Praxis.

(c) Entwerfen Sie in Stichpunkten eine einfache Datenschutz-Folgenabschätzung (DSFA) für eine neue App, die Standort- und Nutzungsdaten verarbeitet. Fassen Sie Ziel, Datenkategorien, potenzielle Risiken, geplante Maßnahmen und Verantwortlichkeiten zusammen.

(d) Begründen Sie, warum Fairness und Gerechtigkeit in digitalen Systemen relevant sind, und nennen Sie zwei typische Konfliktfelder, die sich in Anwendungen der öffentlichen Verwaltung ergeben können.

Aufgabe 3.

(a) Diskutieren Sie die Auswirkungen der Digitalisierung auf Privatsphäre, Autonomie und informationelle Selbstbestimmung in modernen Gesellschaften. Geben Sie zwei konkrete Beispiele.

(b) Beschreiben Sie zentrale Konzepte zu Wissen, Eigentum und Kontrolle im Kontext von digitalen Wissensgütern. Erläutern Sie, wie sich Eigentumsverhältnisse auf Daten und Algorithmen auswirken können.

(c) Analysieren Sie ein Fallbeispiel aus dem Bereich *Smart City*: Eine Kommune plant eine umfangreiche Sensorik für Verkehrsfluss und Luftqualität. Welche gesellschaftlichen Chancen und welche Risiken entstehen hinsichtlich Sicherheit, Privatsphäre und Governance?

(d) Welche Maßnahmen würden Sie vorschlagen, um eine verantwortungsvolle Umsetzung dieses Smart-City-Projekts im Hinblick auf Ethik, Recht und Nachhaltigkeit sicherzustellen?

Aufgabe 4.

(a) Formulieren Sie ein klares Forschungsziel und eine daraus ableitbare Forschungsfrage zu einem aktuellen Thema aus Informatik und Gesellschaft. Begründen Sie die Relevanz der Fragestellung.

(b) Skizzieren Sie eine Vorgehensweise zur Datenerhebung und -auswertung, die sich an ethischen Richtlinien orientiert. Nennen Sie grob geeignete Methoden und deren Vor- und Nachteile.

(c) Erläutern Sie, wie Sie Quellen systematisch prüfen und zitieren würden, und beschreiben Sie ein kurzes Format, das Sie für die Dokumentation der Ergebnisse verwenden.

(d) Reflektieren Sie potenzielle ethische Herausforderungen bei der eigenständigen oder kooperativen Bearbeitung des Themas und benennen Sie entsprechende Gegenmaßnahmen.

Lösungen

Aufgabe 1.

(a) Lösung: Ein soziotechnisches System ist ein Ganzes aus Technik, Menschen, Organisationen und Prozessen, in dem soziale und technische Elemente wechselseitig aufeinander wirken. Es umfasst die Umweltbedingungen, die Normen und Werte der beteiligten Akteurinnen und Akteure sowie die technischen Artefakte, die zur Erreichung bestimmter Ziele eingesetzt werden. Die Grenzen des Systems ergeben sich aus dem Gesamtziel und den relevanten Wechselwirkungen. Typische Merkmale sind Interdependenzen, emergente Eigenschaften und das Vorhandensein von Anpassungs- bzw. Lernprozessen.

Beispiele aus dem Kontext von Informatiksystemen in Organisationen: - Ein Krankenhausinformationssystem (KIS) mit elektronischer Patientenakte, Schnittstellen zu Labor, Abteilungsteams, Pflegeteam und Verwaltung; hier treffen medizinische, rechtliche und organisatorische Anforderungen auf die Technologie. - Ein unternehmensweites ERP-/CRM-System in einem Produktions-/Dienstleistungsunternehmen, das Finanz-, Lager-, Personal- und Kundenprozesse integriert und damit Arbeitsabläufe, Entscheidungswege und Governance beeinflusst.

(b) Lösung: Datenschutz und Transparenz können in der Public-Administration in Konflikt geraten, weil Transparenz oft eine Ausweitung der öffentlichten Einsicht in Entscheidungsprozesse und Daten erfordert, während Datenschutz die Privatsphäre und den Schutz sensibler Informationen sichert. Konfliktfelder ergeben sich insbesondere, wenn Verwaltungsabläufe offengelegt werden sollen (Open Data, Rechenschaftspflicht), aber gleichzeitig personenbezogene Daten geschützt werden müssen.

Zwei daraus resultierende Folgeentscheidungen: - Implementierung eines schichtweiten Datenschutzniveaus: Öffentliche Transparenzberichte und offene Datensätze nur in pseudonymisierter oder aggregierter Form, um individuelle Relationen zu schützen. - Einführung von Datenschutzfolgenabschätzungen (DSFA) und strikter Zugriffskontrollen bei sensiblen Datensätzen, begleitet von Auditprozessen und klaren Reaktionspfaden bei Datenschutzverletzungen.

(c) Lösung: Ethische Dilemmata und Abwägungskriterien bei einer mobilen App, die Standortdaten sammelt, könnten Folgendes umfassen:

Mögliche ethische Dilemmata: - Nutzen vs Privatsphäre: Personalisierte Dienste erhöhen den Nutzen, gehen aber auf Kosten der Privatsphäre und können Verhalten subtil beeinflussen. - Einwilligung vs Notwendigkeit: Erhebung könnte unter Einwilligung legitimiert sein, doch in manchen Fällen könnte der Zweck auch aus praktischer Sicht als notwendig erscheinen. - Zweckbindung vs Funktionsausweitung: Daten, die für eine Funktion gesammelt wurden, könnten später für andere Zwecke genutzt werden (Zweckänderung).

Kriterien zur Abwägung von Konflikten: - Rechtmäßigkeit und Zweckbindung (Art. 5 DSGVO, Rechtsgrundlage Art. 6 ff.) - Verhältnismäßigkeit und Datenminimierung (nur das Nötigste erheben) - Transparenz und Verständlichkeit der Verarbeitung (Betroffene informieren) - Sicherheit der Verarbeitung (Zugriffskontrollen, Verschlüsselung) - Rechenschaft und Möglichkeit der Widerrufsbarkeit (Löschung, Auskunft) - Prüfung auf Diskriminierung oder Benachteiligung (fairness)

(d) Lösung: Die Auswirkungen der genannten Spannungsfelder auf die Gestaltung von IT-Systemen in der Gesellschaft lassen sich so zusammenfassen:

- Zunehmende Verantwortung der Gestalterinnen und Gestalter für ethische Bewertungen von Datennutzung, Transparenzpflichten und Governance. - Notwendigkeit von Ethik-by-Design, Datenschutz-by-Design und Nachhaltigkeitsaspekten in Systemarchitekturen. - Stärkere Rechts- und Regulierungslandschaften mit Prüfvorgaben, Audits und Rechenschaftspflichten, um Ver-

trauen in IT-Systeme zu fördern.

Aufgabe 2.

(a) Lösung: Grundprinzipien der DSGVO im Kontext eines Unternehmens, das digitale Dienste anbietet: - Zweckbindung: Personenbezogene Daten dürfen nur für eindeutig festgelegte, legitime Zwecke verarbeitet werden. - Datenminimierung: Nur die für den Zweck notwendigen Daten erheben. - Richtigkeit: Daten müssen sachlich und aktuell sein. - Speicherbegrenzung: Daten nur so lange speichern, wie es der Zweck erfordert. - Integrität und Vertraulichkeit: Angemessene Sicherheit der Verarbeitung (TOM). - Rechenschaftspflicht: Verantwortliche müssen nachweisen können, dass sie die Vorschriften einhalten.

Drei zentrale Rechte betroffener Personen: - Recht auf Auskunft (Art. 15): Betroffene dürfen Auskunft über verarbeitete Daten erhalten. - Recht auf Berichtigung (Art. 16): Unrichtige Daten müssen berichtigt werden. - Recht auf Löschung (Art. 17): Recht auf "Vergessenwerden" unter bestimmten Bedingungen.

Drei Pflichten von Verantwortlichen: - Rechtmäßige Verarbeitung sicherstellen (Rechtsgrundlage, z. B. Art. 6 ff.; Zweckbindung, Einwilligung). - Technische und organisatorische Maßnahmen (TOM) implementieren (Sicherheit, Datenschutz-by-Design). - Transparenzpflichten und Meldung von Verstöße (Informationspflichten, ggf. Meldung an Aufsichtsbehörden und Betroffene gemäß Art. 33/34).

(b) Lösung: Drei regulatorische Regime, die Einfluss auf IT-Systeme in Deutschland haben, und deren zentrale Auswirkungen:

- DSGVO (EU-weit): Starker Fokus auf Rechtmäßigkeit, Transparenz, Zweckbindung, Minimierung, Rechenschaftspflicht; verlangt DSFA bei Hochrisikoverarbeitung und stärkt Rechte der Betroffenen. - TTDSG (Telekommunikation-Telemedien-Datenschutz-Gesetz): Ergänzt Datenschutz im Bereich der Telekommunikation und Telemedien, insbesondere Regelungen zu Cookies, Tracking und Zugriffen auf Endgeräte; beeinflusst Einwilligungspraxis und Nutzereinwilligungen. - IT-Sicherheitsgesetz 2.0: Stärkere Anforderungen an Betreiber kritischer Infrastrukturen (KRITIS) und Unternehmen mit definierten Sicherheitsstandards; Pflicht zur Meldung von IT-Sicherheitsvorfällen und Umsetzung geeigneter Sicherheitsmaßnahmen.

(c) Lösung: Stichpunkte-Datenbasis einer einfachen DSFA für eine neue App, die Standort- und Nutzungsdaten verarbeitet:

Ziel: Bewertung der Auswirkungen auf Privatsphäre und Grundrechte; Minimierung potenzieller Risiken; Nachweis der Einhaltung gesetzlicher Vorgaben.

Datenkategorien: - Standortdaten in Echtzeit/Präzise Bewegungsprofile - Nutzungsdaten (App-Nutzung, Funktionen, Nutzungszeitraum) - Gerätekennungen (Device ID, OS-Version) - Metadaten (IP-Adresse, Logs)

Verarbeitungszwecke: Personalisierte Dienste, verbessert Vorschläge, Analyse der Nutzungsmuster.

Potenzielle Risiken: Identifikation, Profiling, Überwachung, Missbrauch durch Dritte, Datenverlust, unklare Zweckbindung, Missachtung von Speicherfristen.

Geplante Maßnahmen: - Datenminimierung, Pseudonymisierung/Anonymisierung, Speicherung nur so lange wie nötig - Zweckbindung klar kommunizieren; Einwilligungserklärungen, Widerrufsmöglichkeiten - Starke Zugriffskontrollen, Verschlüsselung im Ruhezustand und während der Übertragung - Privacy-by-Design und regelmäßige Sicherheitsupdates - Datenschutzhinweise, Transparenzberichte, DPIA-Workflow

Verantwortlichkeiten: Datenschutzbeauftragter (DSB), Produktteam/Entwicklung, Sicherheitsteam, Appointment eines Datenschutzkoordinators, regelmäßige Audits.

(d) Lösung: Warum Fairness und Gerechtigkeit in digitalen Systemen relevant sind und zwei

typische Konflikte in Anwendungen der öffentlichen Verwaltung:

- Relevanz: Automatisierte Entscheidungen beeinflussen Zugang zu Leistungen, Ressourcenallokationen und Diskriminerungsrisiken; faire Gestaltung fördert Legitimität, Vertrauen und Rechtskonformität. - Konfliktfelder: 1) Fairness vs Transparenz: Hochgradig komplexe Algorithmen können schwer verständlich sein; Offenlegung von Modellen steht oft im Widerspruch zu Sicherheits- oder Geschäftsgeheimnissen. 2) Gleichbehandlung vs Effizienz: Automatisierte Systeme können Effizienz steigern, aber Ungerechtigkeiten verstärken, z. B. bei Merkmalsverarbeitung, die zu Benachteiligungen bestimmter Gruppen führen kann.

Aufgabe 3.

(a) Lösung: Auswirkungen der Digitalisierung auf Privatsphäre, Autonomie und informationelle Selbstbestimmung:

- Privatsphäre: Zunehmende Datenerhebung via Alltagsgeräte (Smartphones, Sensoren) reduziert den privaten Rückzugsraum; dauerhafte Präsenz von Messdatenbildet neue Formen von Überwachung. - Autonomie: Verfügbare Informationen beeinflussen Entscheidungen, z. B. durch personalisierte Inhalte und Voreinstellungen; Verfügbarkeit von Daten beeinflusst das Selbstbestimmungsrecht. - informationelle Selbstbestimmung: Individuen können zunehmend kontrollieren, welche persönlichen Informationen geteilt werden; datengetriebene Systeme verändern die Art und Weise, wie Entscheidungen getroffen werden (Kontrolle über Datenverwendung).

Zwei konkrete Beispiele: - Smart Speaker/Sprachassistenten sammeln Sprach- und Nutzungsdaten, um Funktionen zu verbessern; potenziell werden diese Daten auch zu Werbezwecken genutzt. - Verkehrsdatenanalyse durch Smart-City-Initiativen, die Bewegungsmuster der Bürgerinnen und Bürger erfassen; dies kann zu besserer Infrastruktur führen, aber auch zu Tracking-Bedenken, falls Daten atypisch aggregiert werden.

(b) Lösung: Zentrale Konzepte zu Wissen, Eigentum und Kontrolle im Kontext digitaler Wissensgüter:

- Wissensgüter: Daten, Algorithmen, Modelle, Inhalte, die Wert schaffen, wenn sie genutzt, weitergegeben oder veredelt werden. - Eigentum: Debatte über Eigentumsrechte an Daten (Datenhoheit), geistiges Eigentum an Algorithmen, Lizenzen, Nutzungsbedingungen; Daten können gemeinschaftlich oder privat genutzt werden. - Kontrolle: Wer darf Daten verwenden, unter welchen Bedingungen, zu welchem Zweck; Einfluss auf Verfügbarkeit, Modifikation und Weiterverwendung.

Auswirkungen von Eigentumsverhältnissen auf Daten und Algorithmen: - Zentralisierte Eigentumsverhältnisse können Monopole schaffen, Zugang zu Daten wird ungleich verteilt, Innovationshemmnisse entstehen. - Open-Source-Modelle und offene Datenformate fördern Transparenz, Reproduzierbarkeit und Kooperation, aber auch Freiheitsgrade bei Missbrauch. - Verträge, Lizenzmodelle und Nutzungsbedingungen steuern, wer Daten interpretieren, weiterverwenden oder kommerzialisieren darf.

(c) Lösung: Fallbeispiel *Smart City*: Kommune plant umfangreiche Sensorik für Verkehrsfluss und Luftqualität.

Chancen: - Verbesserte Verkehrslenkung, reduzierte Staus, effizienterer öffentlicher Nahverkehr. - Frühwarnsysteme für Luftqualitätsprobleme, bessere Stadtplanung, Umweltmonitoring. - Neue Governance-Möglichkeiten durch Bürgerbeteiligung und datengetriebene Entscheidungsprozesse.

Risiken: - Privatsphäre-Verletzungen durch umfangreiche Überwachung; Gefahr der Profilbildung durch Bewegungsdaten. - Sicherheitsrisiken (Datenlecks, Manipulation der Sensorik). - Governance-Herausforderungen: Wer besitzt die Daten? Wer kontrolliert den Zugang? Welche Verantwortlichkeiten bestehen?

(d) Lösung: Maßnahmen für eine verantwortungsvolle Umsetzung dieses Smart-City-Projekts:

- Ethik- und Governance-Rahmen: Ethikkommission, Stakeholder-Engagement, Transparenzberichte. - Datenschutz durch Technik: Minimierung, Pseudonymisierung, Privacy-by-Design, Data Governance mit festen Zugriffsrechten. - Rechtliche Compliance: DSFA, Einhaltung von DSGVO, TTDSG, klare Rechtsgrundlagen für Erhebung und Verarbeitung. - Sicherheit und Resilienz: starke Authentifizierung, regelmäßige Audits, Incident-Response-Pläne, regelmäßige Sicherheitsupdates. - Nachhaltigkeit: Energieeffizienz, Ressourcenverantwortung, Berücksichtigung sozialer

Auswirkungen auf Bürgerinnen und Bürger.

Aufgabe 4.

(a) Lösung: *Forschungsziel:* Untersuchen, wie der Einsatz von KI-gestützten Entscheidungsprozessen in der öffentlichen Verwaltung die Fairness, Transparenz und Rechtsstaatlichkeit beeinflusst. *Forschungsfrage:* Welche Faktoren begünstigen oder behindern faire, transparente und rechtssichere KI-gestützte Entscheidungsprozesse in der öffentlichen Verwaltung, und wie können Governance-Modelle Vertrauen, Rechenschaftspflicht und Rechtskonformität stärken? Begründung der Relevanz: Angesichts zunehmender Automatisierung in Verwaltungsabläufen ist eine verantwortungsvolle Gestaltung notwendig, um demokratische Prinzipien und Gerechtigkeit zu wahren.

(b) Lösung: Vorgehensweise zur Datenerhebung und -auswertung, orientiert an ethischen Richtlinien:

Vorgehen: - Literaturrecherche, Rechtsrahmenanalyse (DSGVO, TTDSG, IT-Sicherheitsgesetz) und Fallstudien. - Empirische Datenerhebung: Experteninterviews mit Verwaltungsmitarbeiterinnen und -mitarbeitern, Fokusgruppen mit Bürgerinnen und Bürgern, ggf. Umfragen.

Methoden (kurz): - Qualitativ: Semi-strukturierte Interviews, Dokumentenanalyse; Vorteil: tiefes Verständnis, Nachteil: geringe Quantität. - Quantitativ: Umfragen, statistische Auswertung; Vorteil: Generalisierbarkeit, Nachteil: superficialität bei komplexen Zusammenhängen. - Mixed-Methods: Kombination beider Ansätze.

Vor- und Nachteile: - Qualitativ: Tiefgang, aber zeitaufwendig; schützt Privatsphäre durch Anonymisierung. - Quantitativ: Breite Abdeckung, aber privilegiert messbare Größen; Bedarf an validen Instrumenten. - Ethik: Zustimmung, Anonymisierung, Minimierung belastender Fragen; Datenschutz bei sensiblen Daten.

(c) Lösung: Vorgehen zur systematischen Quellenprüfung und -zitatierung sowie kurzes Format für die Ergebniss-Dokumentation:

Quellenprüfung: - Relevanzprüfung: Ist die Quelle direkt auf die Forschungsfrage bezogen? - Wissenschaftlichkeit: Peer-Review-Status, Autorenkompetenz, Publikationsort. - Aktualität: Berücksichtigen aktueller Entwicklungen in IT-Sicherheit und Datenschutz. - Bias-Check: Wer finansiert die Studie? Welche potenziellen Interessen beeinflussen die Darstellung?

Zitier-Format (Vorschlag): APA-ähnliches Format, konsistent im Text zitieren (Autor Jahr) und eine am Ende angehängte Literaturliste.

Kurzes Format für die Ergebnisdokumentation (Template): - Titel der Arbeit - Autor/in(nen) - Datum - Zitat (Direkt): [Autor, Jahr, Seite] - Paraphrase: Kurze sinnhafte Zusammenfassung - Relevanz für die Fragestellung - Qualitätskriterien: Evidenzgrad, Methodik, Limitationen

(d) Lösung: Potenzielle ethische Herausforderungen bei der eigenständigen oder kooperativen Bearbeitung des Themas und Gegenmaßnahmen:

Herausforderungen: - Datenschutz und Privatsphäre der Teilnehmenden in Interviews und in Verbindung mit Verwaltungsdaten. - Macht- und Konfliktpotential innerhalb Kooperationsgruppen (ungleiche Beiträge, unklare Autorenschaft). - Risiko von Missbrauch der Forschungsergebnisse (z. B. Weitergabe sensibler Erkenntnisse).

Gegenmaßnahmen: - Ethisches Votum bzw. IRB/Ethikkommission, klare Zustimmungsprozesse, Anonymisierung von Teilnehmenden. - Klare Vereinbarungen zur Mitarbeit, faire Zuwertung von Beiträgen, dokumentierte Autorenschaftsregeln. - Datenmanagementplan: Zugriffsbeschränkungen, Speicherung, Löschung, Versionierung; Offenlegung relevanter Einschränkungen. - Offene Kommunikationskultur, regelmäßige Reflexion zu Bias und Transparenz der Methoden.