Probeklausur

Informatik und Gesellschaft

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

Bearbeitungszeit: 120 Minuten.

Aufgabe 1.

(a) Beschreiben Sie zentrale Begriffe der Ethik in Informatik und der Berufsethik von Informatikerinnen.

(b) Nennen Sie drei typische ethische Dilemmata, die in IT-Systemen auftreten können, und skizzieren Sie eine allgemeine Vorgehensweise zur Abwägung.

(c) Welche Stakeholder-Gruppe(n) sind in Entscheidungsprozessen rund um digitale Systeme typischerweise beteiligt? Beschreiben Sie deren jeweilige Perspektive.

(d) Welche Pflichten ergeben sich aus gesellschaftlicher Verantwortung fur Informatikerinnen und Informatiker? Erwägen Sie den Bezug zu Transparenz, Rechenschaftspflicht und Konfliktpotenzialen.

Aufgabe 2.

(a) Unterschied zwischen Datenschutz und Datensicherheit: Definieren Sie beide Begriffe und diskutieren Sie, wie sie sich gegenseitig ergänzen.

(b) Skizzieren Sie ein praxisnahes Datenschutzkonzept fur eine Webanwendung, das Grundprinzipien wie Zweckbindung, Minimierung und Transparenz berücksichtigt.

(c) Welche zentralen Rechte der Nutzenden bestehen im EU-Datenschutzrecht und wie können sie praktisch umgesetzt werden?

(d) Diskutieren Sie grob Kosten und Nutzen von Datenschutzmaßnahmen in einem mittleren Unternehmen im Kontext von Geschäftsprozessen und Innovationsdruck.

Aufgabe 3.

(a) Was bedeutet Fairness in der algorithmischen Entscheidungsfindung und welche Ziele verfolgt der Begriff in diesem Kontext?

(b) Nennen Sie zwei typische Bias-Arten, die in Modellen auftreten können, und geben Sie je ein Beispiel.

(c) Beschreiben Sie drei konkrete Optionen, um Fairness in einer Entscheidungsmaschine zu fördern (zwei technische, eine organisatorische Maßnahme).

(d) Diskutieren Sie, wie Transparenz, Rechenschaftspflicht und Beteiligung der Betroffenen bei der Gestaltung von IT-Systemen berücksichtigt werden können.

Aufgabe 4.

(a) Analysieren Sie Spannungsfelder zwischen Digitalisierung und Nachhaltigkeit. Berücksichtigen Sie ökologische, ökonomische und soziale Dimensionen.

(b) Geben Sie ein kurzes Fallbeispiel einer digitalen Anwendung, in dem ethische oder regulatorische Fragestellungen relevant sind, und erläutern Sie, welche Aspekte beurteilt werden müssen.

(c) Erläutern Sie einen einfachen Prozess, wie Teams eigenständig ein aktuelles gesellschaftlich relevantes Thema identifizieren, analysieren und wissenschaftlich belegen können.

(d) Beschreiben Sie, wie die Ergebnisse einer solchen Analyse thematisch und formell aufbereitet und kommuniziert werden können.

Lösungen

Bearbeitungszeit: 120 Minuten.

Aufgabe 1.

(a) Lösung:
Ethik in Informatik befasst sich mit dem moralischen Handeln im Umgang mit Informationstechnik, Daten und Systemen. Zentrale Begriffe sind:

- Autonomie und Privatsphäre der Nutzenden,
- Nicht-Schädigung (Honoring the principle of non-maleficence) und Wohlergehen der Betroffenen,
- Gerechtigkeit und Fairness (gleiche Berücksichtigung von Interessen, Abbau von Diskriminierung),
- Transparenz und Nachvollziehbarkeit von Entscheidungen,
- Verantwortlichkeit und Rechenschaftspflicht der Entwicklerinnen und Entwickler sowie der Organisationen,
- Datenschutz und Datensicherheit als konkrete Schutzmechanismen.

Die Berufsethik der Informatikerinnen umfasst normative Prinzipien wie Verantwortung, Integrität, Qualität, Sorgfaltspflicht, Offenlegung von relevanten Informationen gegenüber Stakeholdern sowie das Streben nach Safe-by-Design und Responsible AI. Ethik und Berufsethik unterscheiden sich dahingehend, dass Ethik allgemein moralische Prinzipien adressiert, während Berufsethik auf die Pflichten und Standards in beruflichen Kontexten abzielt (Codices, normative Orientierung im Arbeitsalltag).

(b) Lösung:
Drei typische ethische Dilemmata in IT-Systemen:

- Privatsphäre vs. Nutzen durch Datennutzung (z. B. Personalisiertes Marketing vs. umfassende Datenerhebung),
- Transparenz vs. geschäftliche Geheimhaltung (Offenlegung von Algorithmen vs. Wettbewerbsschutz),
- Automatisierung vs. Arbeitsplatzsicherung (Effizienzsteigerung vs. Beschäftigungssicherung und faire Übergänge).

Allgemeine Vorgehensweise zur Abwägung:

- Werte identifizieren: Welche Prinzipien stehen zur Debatte (Privatsphäre, Sicherheit, Fairness, Transparenz, Profit, Innovation)?
- Stakeholder-Analyse: Wer ist betroffen, welche Interessen haben sie, welche Rechte gelten?
- Optionen erzeugen: Mehrere Lösungswege mit unterschiedlicher Gewichtung der Werte.
- Kriterien festlegen: Welche Kriterien (Rechtmäßigkeit, Auswirkungen auf Betroffene, Nachhaltigkeit) sind entscheidend?
- Bewertung vornehmen: Nutzen-Kosten-Analyse, Risikoeinschätzung, Fairness- und Gleichbehandlungsaspekte prüfen.

- Rechenschaft und Dokumentation: Entscheidungsprozesse transparent machen, Begründungen nachvollziehbar festhalten.
- Iteration und Revision: Ergebnisse regelmäßig überprüfen und an neue Informationen anpassen.

(c) Lösung:
Typische Stakeholder-Gruppen und deren Perspektiven:

- Nutzende/Betroffene: Privatsphäre, Datenschutz, Zugänglichkeit, Benutzbarkeit, Mitspracherecht.
- Entwickelnde und Betreiberinnen: Machbarkeit, Sicherheit, Wartbarkeit, Kosten, Compliance.
- Unternehmen bzw. Eigentümerinnen: wirtschaftlicher Erfolg, Haftung, Risiko- und Reputationsmanagement.
- Regulierungsbehörden und Gesetzgeber: Rechtskonformität, Datenschutz, Verbraucherschutz, Transparenzanforderungen.
- Zivilgesellschaft, Wissenschaft und Medien: Transparenz, Rechenschaft, ethische Standards, kritische Begleitung.
- Mitarbeitende: Arbeitsbedingungen, Sicherheit, Fortbildung, Mitbestimmung.

Perspektiven: Nutzende benötigen klare Informationen und Kontrolle über ihre Daten; Entwicklerinnen benötigen klare Vorgaben und Regeln; Regulatorik zielt auf Schutz und Fairness; Gesellschaftliche Akteursgruppen fordern Rechenschaft und Missbrauchsprävention.

(d) Lösung:
Pflichten aus gesellschaftlicher Verantwortung für Informatikerinnen:

- Transparenz: Offenlegung von Kriterien, Entscheidungslogik und relevanten Annahmen, soweit zulässig.
- Rechenschaftspflicht: Dokumentation von Entscheidungen, Auditierbarkeit von Systemen, Verantwortungszuweisung.
- Konfliktpotenziale: Governance-Strukturen, Ethik-Boards, Ombudsmänner/-frauen, Mechanismen zur Meldung von Missständen.
- Sicherheit und Privatsphäre als Grundpflicht: Datenschutzkonzepte, Sicherheitsarchitektur, Risikomanagement.
- Verantwortung gegenüber Gesellschaft: Nachhaltigkeit, Zugangsgerechtigkeit, Vermeidung von Diskriminierung.
- Ethik by Design: Berücksichtigung ethischer Kriterien in der Entwicklung, regelmäßige Evaluierung und Anpassung.

Aufgabe 2.

(a) Lösung:
Datenschutz und Datensicherheit sind zwei eng verwandte, aber unterschiedliche Konzepte:

- Datenschutz: Rechts- und ethische Frage, wer welche Daten zu welchem Zweck verwenden darf. Kernelemente sind Zweckbindung, Datenminimierung, Transparenz, Einwilligung, Widerspruchsrechte und das Recht auf Information.
- Datensicherheit: Technische und organisatorische Maßnahmen zum Schutz von Daten vor Verlust, Missbrauch, unbefugtem Zugriff und Beschädigung (z. B. Verschlüsselung, Zugriffskontrollen, Backup, Incident Response).

Sie ergänzen sich, denn gute Datenschutzpraktiken lassen sich nur umsetzen, wenn die Daten auch sicher verwaltet werden; umgekehrt erhöht eine robuste Datensicherheit den tatsächlichen Datenschutz, indem sie Verstöße und unbefugte Verarbeitung verhindert.

(b) Lösung:
Praxisnahes Datenschutzkonzept für eine Webanwendung (Prinzipien Zweckbindung, Minimierung, Transparenz):

- Dateninventar und Rechtsgrundlagen: Welche Daten werden erhoben? Welche Rechtsgrundlage (Einwilligung, Vertrag, berechtigtes Interesse)?
- Zweckbindung und Minimierung: Nur Daten erheben, die für den jeweiligen Zweck notwendig sind.
- Transparenz: Datenschutzerklärung, klare Nutzerinformationen, verständliche Einwilligungsprozesse.
- Rechte der Nutzenden: Mechanismen zur Auskunft, Berichtigung, Löschung, Widerspruch, Datenübertragbarkeit.
- Auftragsverarbeitung/Third-Party: Verträge zur Auftragsverarbeitung, Prüfung der Drittanbieter-Datentransfers.
- Technische Maßnahmen: Pseudonymisierung, Minimierung der gespeicherten Daten, TLS-Transport, sicheres Cookies-Management, regelmäßige Penetrationstests.
- Data Governance: Data Retention Policy, regelmäßige DSFA (Datenschutz-Folgenabschätzung) bei risikoreichen Verarbeitungen.
- Incident Response: Verfahren bei Datenschutzverletzungen, Meldung innerhalb gesetzlicher Fristen.

(c) Lösung:
Zentrale Rechte der Nutzenden im EU-Datenschutzrecht (DSGVO) und praktische Umsetzung:

- Recht auf Auskunft und Berichtigung: Nutzende können über Alle Daten, Verarbeitungszwecke und Kategorien Auskunft verlangen; Berichtigung fehlerhafter Daten.
- Recht auf Löschung (Recht auf Vergessenwerden): Daten bei berechtigtem Antrag löschen, sofern keine gesetzlichen Aufbewahrungspflichten greifen.

- Recht auf Einschränkung der Verarbeitung, Widerspruch und Widerruf der Einwilligung: Mechanismen zur Abwicklung, explizite Deaktivierung.
- Recht auf Datenübertragbarkeit: Daten in maschinenlesbarem Format übertragen, Anbieterwechsel erleichtern.
- Automatisierte Entscheidung/Profiling: Transparenz über Kriterien, ggf. menschliche Prüfung.

Praktische Umsetzung:

- Ein integriertes Self-Service-Portal für Auskunft, Berichtigung, Löschung und Datenexport.
- Klare Datenschutzerklärungen und verständliche Einwilligungsdialoge.
- Technische Umsetzung von Rechten (z. B. Lösch- und Export-APIs, Audit-Logs).
- Benennung eines Datenschutzbeauftragten, falls gesetzlich vorgeschrieben; DPIAs bei risikoreichen Verarbeitungen.

(d) Lösung:
Kosten und Nutzen von Datenschutzmaßnahmen in einem mittelständischen Unternehmen:

- Kosten: Implementierung technischer Lösungen (Verschlüsselung, Zugangskontrollen), Personal (DSMS, DPIAs, Schulungen), laufende Audits, Dokumentation, potenzielle Verzögerungen bei Markteinführungen.
- Nutzen: Risikominderung bei Bußgeldern und Reputationsverlust, Vertrauensgewinn bei Kundinnen und Kundinnen, bessere Datenqualität, Potenzial für neue Geschäftsfelder durch datenschutzfreundliche Systeme.
- Im Kontext von Geschäftsprozessen und Innovationsdruck: Abwägen von Geschwindigkeit vs. Sicherheit; Einsatz von Privacy-by-Design als Beschleuniger, da spätere Nachbesserungen teurer sind. Kosten-Nutzen-Analysen sollten auch Opportunitätskosten von Nicht-Handeln berücksichtigen.

Aufgabe 3.

(a) Lösung:
Fairness in der algorithmischen Entscheidungsfindung bedeutet, dass Entscheidungen gerecht, transparent und ohne unbegründete Benachteiligung getroffen werden. Ziele:

- Diskriminierungsfreiheit und Chancengleichheit,
- Berücksichtigung relevanter Merkmale bei der Modellierung (oder bewusste Entkoppelung sensibler Merkmale),
- Gleichbehandlung von Gruppen, die durch historische Verzerrungen benachteiligt wurden, ohne systematisch neue Ungleichheiten zu erzeugen.

Typische Präzisionsziele sind demographische Gleichstellung, Kalibrierung der Wahrscheinlichkeiten, oder Gleichheit der Auswirkungen (outcome fairness); je nach Kontext können unterschiedliche Formaldefinitionen (z. B. Demographic Parity, Equalized Odds, Calibration) gewählt werden.

(b) Lösung:
Zwei typische Bias-Arten mit Beispielen:

- Repräsentations-Bias (Sampling Bias): Ein Modell zur Kreditvergabe wird mit historischen Daten trainiert, in denen bestimmte Gruppen aufgrund früherer Diskriminierung unterrepräsentiert sind; das Modell erlernt diese Verzerrung.
- Proxy-/Merkmal-Bias: Ein Modell nutzt ein Proxy-Attribut (z. B. Postleitzahl als Proxy für sozioökonomischen Status), das mit einer geschützten Eigenschaft korreliert; das führt zu indirekter Diskriminierung.

(c) Lösung:
Drei konkrete Optionen, um Fairness in einer Entscheidungsmaschine zu fördern:

- Technisch (vorbereitend): Pre-processing-Ansätze wie Re-Sampling, Reweighting oder Fair Representation Learning, um verzerrte Verteilungen zu korrigieren; Nutzung von Fairness-Aware-Algorithmen.
- Technisch (nachbereitend): Post-processing-Methoden wie Schwellenwertanpassung (threshold tuning) oder Justierung der Entscheidungsgrenzen, um disparate Impact zu reduzieren (z. B. Equalized Opportunities).
- Organisatorisch: Diverses Team-Setup, Governance-Strukturen, regelmäßige Ethik-Reviews und Stakeholder-Beteiligung, Transparenz gegenüber Betroffenen, klare Richtlinien zur Responsible AI.

(d) Lösung:
Berücksichtigung von Transparenz, Rechenschaftspflicht und Beteiligung der Betroffenen:

- Transparenz: Modell- und Datendokumentation (Datasheets, Model Cards), verständliche Erklärungen der Entscheidungslogik.
- Rechenschaftspflicht: Verantwortlichkeiten definieren, Audits planen, externe Prüfungen ermöglichen, Nachvollziehbarkeit der Entscheidungen sicherstellen.

- Beteiligung der Betroffenen: Einbindung betroffener Gruppen in Design-Reviews, Feedback-Kanäle, Mitbestimmung bei relevanten Entscheidungen, Mechanismen zur Beschwerde und redress.

Aufgabe 4.

(a) Lösung:
Spannungsfelder zwischen Digitalisierung und Nachhaltigkeit:

- Ökologische Dimension: Energieverbrauch von Rechenzentren, Lebenszyklus von Hardware, E-Waste, Ressourcenverbrauch bei der Herstellung von Geräten.
- Ökonomische Dimension: Erstinvestitionen in grüne Infrastruktur vs. laufende Betriebskosten, Langzeit-RoI von Nachhaltigkeitsmaßnahmen, Regulierungskosten.
- Soziale Dimension: Digitale Spaltung, Zugang zu digitalen Dienstleistungen, Auswirkungen auf Arbeiten und Beschäftigung, faire Verteilung von Vorteilen und Nachteilen.

Die Balance erfordert Strategien wie Energieeffizienz, erneuerbare Energien, Kreislaufwirtschaft, verantwortungsvolles Data-Management und gerechte Verteilung der Zugänge zu digitalen Diensten.

(b) Lösung:
Fallbeispiel: KI-gestützte Personalrekrutierung (Hiring Tool) oder datengetriebenes Energiemanagement in einer Stadt. Relevante ethische oder regulatorische Fragestellungen:

- Diskriminierungspotential und Faire Behandlung von Bewerbergruppen,
- Transparenz der Entscheidungslogik und Erklärbarkeit gegenüber Betroffenen,
- Datenschutz und Datensicherheit der Personal- bzw. Nutzungsdaten,
- Rechtskonformität (DSGVO, Antidiskriminierungsgesetze, ggf. spezifische Regulierung für KI-Anwendungen),
- Umwelt- und Ressourceneffizienz der IT-Infrastruktur, Energieverbrauch der Modelle.

Beurteilungsaspekte: Auswirkungen auf Betroffene, Rechtmäßigkeit, Fairness, Erklärbarkeit, Sicherheitsniveau, Umweltfolgen, Compliance-Risiken.

(c) Lösung:
Einfacher Prozess, wie Teams eigenständig ein aktuelles gesellschaftlich relevantes Thema identifizieren, analysieren und wissenschaftlich belegen können:

- Themen-Scan: Forschungs- und Marktanalyse, Stakeholder-Inputs, regulatorische Entwicklungen.
- Problemdefinition: Klarer Rahmen, relevante Fragestellungen, Zielsetzung.
- Datenerhebung und Analyse: Sammlung geeigneter qualitativer/quantitativer Daten, methodische Analyse (Fallstudien, Literatur, Datenanalyse).
- Optionen generieren: Mehrere Handlungsoptionen mit Vor- und Nachteilen.
- Bewertung: Kriterienbasierte Bewertung, ethische Abwägung, Nachhaltigkeitsaspekte.
- Belegung: Erstellung einer wissenschaftlich belegten Beurteilung (Quellen, Evidenz, Limitationen).

(d) Lösung:
Aufbereitung und thematische/formelle Kommunikation der Ergebnisse:

- Struktur: Einleitung, Methodik, Ergebnisse, Diskussion, Schlussfolgerungen, Ausblick.
- Wissenschaftliche Belege: Quellenangaben, Zitate, Datenverfügbarkeit, Reproduzierbarkeit der Analysen.
- Darstellung: Klare Sprache, verständliche Grafiken, Executive Summary für Entscheidungsträger.
- Stakeholder-spezifische Kommunikation: Technische Details für Fachpublikum, ethische und regulatorische Implikationen für Policymaker, kompakte Zusammenfassung für Management.
- Governance und Nachverfolgung: Empfehlungen, Verantwortlichkeiten, Zeitplan, Messgrößen zur Nachprüfung.