

Algoritmin perusteet ja tekoälyn etiikka -kurssi: Teoriasta käytäntöön

Työkalupakki synkronisille luennoille

**Osaamiskokonaisuus 2 | Tekoälyn
yksityisyys ja käytettävyys**
PowerPoint-diat tueksi

SISÄLLYS

- JOHDANTO - 3
- YKSITYISYYDEN JA KÄYTETTÄVYYDEN YMMÄRTÄMINEN
TEKOÄLYSSÄ- 9
- TIETOSUOJAN TÄRKEIMMÄT SEIKAT- 24
- YKSITYISYYDEN JA KÄYTETTÄVYYDEN VUOROVAIKUTUS - 39
- YKSITYISYYDEN JA KÄYTETTÄVYYDEN MERKITYS - 45
- RISKIT JA HYÖDYT - 51
- TAPAUSTUTKIMUS: TEKOÄLY VALVONNASSA - 56
- JOHTOPÄÄTÖS - 65

JOHDANTO



IMAGE SOURCE | Generated by DALL-E

TÄSTÄ OSAAMISKOKONAISUUDESTA LÖYDÄT SEURAAVAT AIHEET:

- Ymmärtää tekoälyn yksityisyyden ja käytettävyyden monimutkaisen suhteen.
- Tutkia tietosuojan peruselementtejä.
- Analysoida, miten yksityisyys ja käytettävyys vaikuttavat toisiinsa ja tekoälyjärjestelmiin.
- Korostaa yksityisyyden ja käytettävyyden merkitystä tekoälysovelluksissa.
- Arvioida tekoälyn yksityisyyteen ja käytettävyyteen liittyviä potentiaalisia riskejä ja etuja.
- Tutkia todellista tapaustutkimusta: tekoälyn käyttöönotto valvontajärjestelmissä.

OSAAMISKOKONAISUUDEN LOPUSSA OSAAT:

- Ymmärtää tekoälyjärjestelmien yksityisyyden ja käytettävyyden monimutkaisen suhteen ja tunnistaa näiden kahden näkökohdan tasapainottamisen merkityksen vastuullisen tekoälyn käyttöönotolle.
- Tunnistaa tietosuojan olennaiset osatekijät, kuten suostumus, käyttötarkoituksen rajoittaminen ja turvallisuus.
- Analysoida, miten yksityisyys ja käytettävyys kohtaavat tekoälysovelluksissa ja johtavat eettisiin ongelmiin.
- Arvioida sekä tekoälyteknologioihin liittyvät potentiaaliset riskit, kuten tietoturvaloukkaukset ja vinoumat, että niiden edut, kuten tehokkuuden kasvu ja käyttökokemuksen parantuminen.

On suositeltavaa esitellä kiinnostava kysymys tai yllättävä fakta, joka herättää oppijoiden mielenkiinnon nykyisen tekoälyn tilanteen selittämiseen ja korostaa yksityisyyden ja käytettävyyden merkitystä

(katso seuraavat diat esimerkkejä kysymyksistä).

KYSYMYKSET

”Mitä palveluita käytät, joiden tiedät keräävän tietojasi toiminnallisuuden parantamiseksi ja käyttökokemuksen mukauttamiseksi?”

Älypuhelimet|| Sosiaalisen median alustat|| Suoratoistopalvelut|| Verkkokauppasivustot|| Älykotilaitteet|| Kuntoseurantalaitteet ja terveyssovellukset|| Ääniohjaus|| Navigointi- ja matkasovellukset|| Pankki- ja rahoitussovellukset

KYSYMYKSET

”Kuinka hyvin hyväksyt, että nämä palvelut keräävät henkilötietojasi?”

Erittäin hyvä || Melko hyvä || Neutraali || Melko huono || Erittäin huono

YKSITYISYYDEN JA KÄYTETTÄVYYDEN YMMÄRTÄMINEN TEKOÄLYSSÄ



IMAGE SOURCE | Generated by DALL-E

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä



IMAGE SOURCE | Generated by DALL-E

Sarahin dilemma: yksityisyyden ja käytettävyyden välinen kompromissi

Opiskelija Sarah käyttää älylaitteita käytettävyyden vuoksi, mutta on huolissaan siitä, miten laitteet keräävät ja käyttävät hänen henkilötietojaan. Tämä korostaa tekoälyn ja yksityisyyden välistä herkkää tasapainoa.

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä

KYSYMYS

"Luuletko, että Sarah otti huomioon yksityisyyden suojan ennen näiden laitteiden ostamista?"

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä

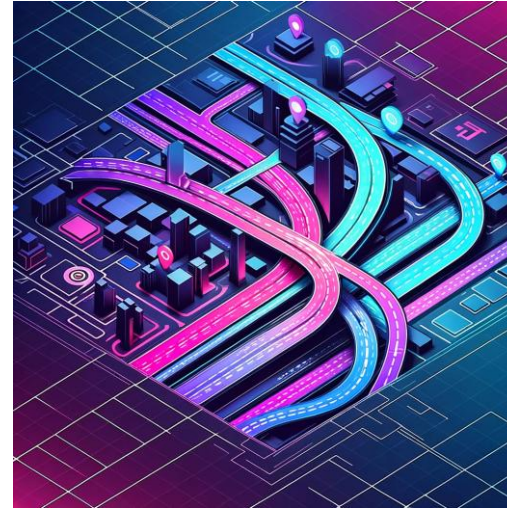


Tässä on Sarah, opiskelija, joka haluaa yksinkertaistaa elämänsä älykkään teknologian avulla.



Sarahin älykäs elämä

Älykaiutin päivittäisiin aikatauluihin ja viihteeseen, älytermostaatti optimaalisiin elinolosuhteisiin ja älykello kuntoilun seurantaan.



Käytettävyys parhaimmillaan

"Eräänä aamuna Sarahin älykaiutin ehdottaa hänelle uuden reitin ruuhkien välttämiseksi – täydellinen esimerkki tekoälyn tarjoamasta käytettävyydestä."



Kun käytettävyys muuttuu

henkilökohtaiseksi

"Myöhemmin henkilökohtainen mainos suosittelee hänelle hänen suosikkilatteaan läheisestä kahvilasta."

IMAGES SOURCE | Generated by DALL-E

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä

KYSYMYS

Mitä mieltä olet laitteista, jotka tekevät päätöksiä päivittäisten rutiiniesi perusteella? Mitkä ovat mahdolliset yksityisyyden suojan haitat?

Mitä tietoja on voitu jakaa tämän mainoksen personointia varten? Oletko tyytyväinen tähän tietojen jakamisen tasoon personoitujen mainosten osalta?

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä



Yhteyksien luominen

Sarahin laitteet mukautuvat hänen tapoihinsa ja aikatauluunsa, mikä osoittaa älyteknologian invasiivisen mutta saumattoman integroinnin.



Käytettävyyden kääntöpuoli

"Sarah arvostaa tehokkuutta, mutta on huolissaan siitä, kuinka paljon henkilökohtaisia tietoja hänen laitteensa keräävät ja käyttävät ilman hänen nimenomaista suostumustaan."



Yksityisyys vs. käytettävyys

Tehokkuus ja henkilökohtaiset palvelut vs. yksityisyyden menetys ja tietojen luvaton käyttö.



"Miten Sarahin pitäisi mielestäsi käsitellä yksityisyyttä koskevat huolenaiheensa?"

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä

KYSYMYS

Onko teknologia koskaan saanut sinut tuntemaan samoin kuin Sarah? Mitä toimia olet mahdollisesti toteuttanut?

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä

KYSYMYS

Mitä neuvoisit Sarahille tässä tilanteessa? Mitä hän voi tehdä hallitakseen tietojaan paremmin?

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä

Mitä on yksityisyys?

"Yksityisyys on perusihmisoikeus, joka on tunnustettu YK:n ihmisoikeuksien julistuksessa, kansalaisoikeuksia ja poliittisia oikeuksia koskevassa kansainvälisessä yleissopimuksessa sekä monissa muissa kansainvälisissä ja alueellisissa sopimuksissa."

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä

Tekoälyn yhteydessä yksityisyys käsittää useita **keskeisiä ulottuvuuksia**:

Tietosuoja	+
Tietoturva	+
Henkilökohtainen autonomia	+

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä

Tekoälyn yhteydessä yksityisyys käsittää useita **keskeisiä ulottuvuuksia**:

Tietosuoja

-

Tietosuoja suojaa henkilötietoja luvattomalta käytöltä tai paljastamiselta ja varmistaa, että yksilöt voivat hallita tietojaan mieltymystensä ja säännösten mukaisesti. Tekoälyssä henkilötietojen suojaaminen on välttämätöntä rikkomusten ja väärinkäytön estämiseksi, mikä on ratkaisevan tärkeää järjestelmän luotettavuuden kannalta. GDPR:n kaltaiset säännökset asettavat tiukat ohjeet tietojen keräämiselle, käsittelylle ja tallentamiselle, ja niiden tarkoituksena on suojata yksityisyyden suoja ja varmistaa vastuuvollisuus.

Esimerkki: Kuvittele terveyssovellus, joka tallentaa lääketieteellisiä tietoja ilman suostumusta tai turvatoimenpiteitä. Ilman salausta se altistuu tietoturvaloukkauksille, joissa arkaluonteisia tietoja voi paljastua. GDPR-asetuksen noudattamatta jättäminen, kuten luvaton tietojen jakaminen, voi johtaa oikeudellisiin seuraamuksiin, mikä korostaa vahvan tietosuojan tarvetta tekoälyssä.

Tietoturva

+

Henkilökohtainen autonomia

+

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä

Tekoälyn yhteydessä yksityisyys käsittää useita **keskeisiä ulottuvuuksia**:

Data privacy



Tietoturva

Tietoturva käsittää suojatoimenpiteitä, joilla varmistetaan, että tiedot pysyvät suojattuina vioittumiselta ja luvattomalta käytöltä sekä säilyttävät eheydensä ja luottamuksellisuutensa.

Tekoälyjärjestelmissä käytettyjen tietojen suojaamiseksi hakkeroinnilta ja vuodoilta tarvitaan vankkoja turvallisuusprotokollia. Erityisiä turvallisuustoimenpiteitä ovat salaus, joka sekoittaa tiedot niin, että ne ovat lukukelvottomia ilman oikeaa salausavainta, kaksivaiheinen todennus, jossa käyttäjien on annettava kaksi todentamistapaa päästäkseen tietoihin, sekä turvalliset tietojen tallennusratkaisut, kuten salatut tietokannat tai pilvitallennus, jossa on tiukat pääsynvalvontatoimenpiteet.

Esimerkki: Kuvitellaan tilanne, jossa terveydenhuollon tekoälyjärjestelmässä ei ole riittävät turvatoimet. Hakkerit hyödyntävät järjestelmän haavoittuvuuksia päästäkseen luvatta potilastietoihin, mikä johtaa massiiviseen tietovuotoon. Tämän seurauksena arkaluonteiset lääketiedot paljastuvat, mikä johtaa yksityisyyden loukkauksiin, oikeudellisiin seuraamuksiin ja organisaation maineen vahingoittumiseen. Tämä tapaus korostaa, kuinka tärkeää on toteuttaa vankat tietoturvatoimenpiteet tekoälyjärjestelmissä tietovuotojen riskin vähentämiseksi ja arkaluonteisten tietojen suojaamiseksi.

Henkilökohtainen autonomia



Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä

Tekoälyn yhteydessä yksityisyys käsittää useita **keskeisiä ulottuvuuksia**:

Tietosuoja	+
Tietoturva	+
Henkilökohtainen autonomia Henkilökohtainen autonomia tarkoittaa yksilön oikeutta hallita omia henkilötietojaan ja päättää niiden käytöstä. Tekoälyn yhteydessä henkilökohtaisen autonomian kunnioittaminen on ratkaisevan tärkeää yksilön oikeuksien kunnioittamiseksi ja teknologian eettisen käytön varmistamiseksi. Eettisissä tekoälyn käytänteissä etusijalla on tietoon perustuvan suostumuksen saaminen yksilöiltä ennen heidän tietojensa keräämistä ja käyttöä. Tekoälyjärjestelmät voivat vaikuttaa henkilökohtaiseen autonomiaan tekemällä päätöksiä yksilöiden puolesta ilman heidän nimenomaista suostumustaan tai tietämystään. Esimerkki: Tekoälypohjainen työnhakijoiden seulontatyökalu analysoi hakijoiden ansioluetteloita ennustaakseen heidän sopivuuttaan tiettyyn tehtävään, mikä voi vaikuttaa rekrytointipäätöksiin. Eettisiä ongelmia syntyy, jos algoritmi syrjii tai käyttää vinoumia tietoja, mikä heikentää hakijoiden autonomiaa ja edellyttää ihmisen valvontaa.	-

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä

GDPR:n mukaiset tietosuojan keskeiset periaatteet

- Laillisuus, oikeudenmukaisuus ja läpinäkyvyys: henkilötietojen käsittelyn on oltava laillista, oikeudenmukaista ja läpinäkyvää rekisteröityä kohtaan.
- Käyttötarkoituksen rajoittaminen: tiedot on kerättävä tiettyjä, nimenomaisia ja laillisia tarkoituksia varten, eikä niitä saa käsitellä tavalla, joka on yhteensopimaton näiden tarkoitusten kanssa.
- Tietojen minimointi: vain käsittelyn kannalta välttämättömät tiedot kerätään ja käsitellään.
- Tarkkuus: henkilötietojen on oltava paikkansapitäviä ja ajantasaisia; virheelliset tiedot on poistettava tai oikaistava viipymättä.
- Säilyttämisen rajoittaminen: henkilötiedot on säilytettävä muodossa, joka mahdollistaa rekisteröityjen tunnistamisen vain niin kauan kuin se on tarpeen henkilötietojen käsittelytarkoituksen kannalta.
- Tarkkuus ja luottamuksellisuus: tiedot on käsiteltävä tavalla, joka varmistaa asianmukaisen turvallisuuden, mukaan lukien suojaaminen luvattomalta tai laittomalta käsittelyltä sekä vahingossa tapahtuvalta menettämiseltä, tuhoamiselta tai vahingoittumiselta.
- Vastuullisuus: rekisterinpitäjä on vastuussa kaikkien muiden tietosuojaperiaatteiden noudattamisesta ja sen on voitava osoittaa tämä.

Yksityisyyden ja käytettävyyden ymmärtäminen tekoälyssä

Tietosuoja-rikkomus tekoälyjärjestelmässä

Kuvitellaan tilanne, jossa teknologiayritys on kehittänyt tekoälyyn perustuvan terveyden seurantaan tarkoitetun sovelluksen. Sovellus kerää laajasti käyttäjien terveystietoja, kuten sydämen sykettä, uniryhmiä ja verenpainetta. Vaikka kyseessä on arkaluontoista tietoa, tietoturvatoinenpitemet oli laiminlyöty – erityisesti sovelluksen API-rajapinta oli jätetty suojaamatta. Tämä haavoittuvuus johti merkittävään tietovuotoon, jonka seurauksena tuhansien käyttäjien terveystiedot päätyivät väärin käsiin. Vuotanut tieto sisälsi yksityiskohtia, jotka mahdollistivat yksityisyyden loukkaukset ja mahdollisen henkilöllisyyden väärinkäytön. Tietovuodon seurauksena yritys joutui maksamaan merkittävät sakot GDPR-asetuksen rikkomisesta, koska se ei ollut riittävästi suojannut käyttäjien tietoja. Lisäksi tapaus aiheutti vakavaa vahinkoa yrityksen maineelle ja johti käyttäjien luottamuksen menetykseen.

TIETOSUOJAN TÄRKEIMMÄT SEIKAT



IMAGE SOURCE | Generated by DALL-E

Tietosuojan tärkeimmät seikat

Ongelman määrittely ja liiketoiminnan ymmärtäminen

Huomioon otettavat eettiset periaatteet

Suostumus

Click cards to flip ↻

Käyttötarkoituksen
rajoittaminen

Click cards to flip ↻

Tietojen minimointi

Click cards to flip ↻

Turvallisuus

Click cards to flip ↻

Läpinäkyvyys

Click cards to flip ↻

Pääsy ja oikaisu

Click cards to flip ↻

Vastuullisuus

Click cards to flip ↻

Tietosuojan tärkeimmät seikat

Ongelman määrittely ja liiketoiminnan ymmärtäminen

Huomioon otettavat eettiset periaatteet - Suostumus

Yksilöiden suostumuksen hankkiminen ennen heidän tietojensa käyttöä analysointitarkoituksiin on ratkaisevan tärkeää heidän yksityisyytensä ja itsemääräämisoikeutensa kunnioittamiseksi. Pyytämällä nimenomaista lupaa organisaatiot varmistavat, että yksilöt ovat tietoisia siitä, miten heidän tietojensa käytetään, ja voivat tehdä tietoon perustuvia päätöksiä tietojensa jakamisesta.



Käyttötarkoituksen rajoittaminen

Click cards to flip

Tietojen minimointi

Click cards to flip

Turvallisuus

Click cards to flip

Läpinäkyvyys

Click cards to flip

Pääsy ja oikaisu

Click cards to flip

Vastuullisuus

Click cards to flip

Tietosuojan tärkeimmät seikat

Ongelman määrittely ja liiketoiminnan ymmärtäminen

Huomioon otettavat eettiset periaatteet - Käyttötarkoituksen rajoittaminen

Consent

Tarkoituksen rajoittamisen periaatteen noudattaminen tarkoittaa, että tietoja käytetään vain määriteltyihin ja laillisiin analyttisiin tarkoituksiin. Määrittelemällä selkeästi tietojen käyttötarkoituksen organisaatiot estävät henkilötietojen väärinkäytön tai luvattoman jakamisen ja turvaavat siten

yksilöiden yksityisyyden suojaa.

Data minimization

Click cards to flip ↻

Security

Click cards to flip ↻

Transparency

Click cards to flip ↻

Access and correction

Click cards to flip ↻

Accountability

Click cards to flip ↻

Tietosuojan tärkeimmät seikat

Ongelman määrittely ja liiketoiminnan ymmärtäminen

Huomioon otettavat eettiset periaatteet - Tietojen minimointi

Consent

Purpose limitation

Vain välttämättömien tietojen kerääminen ja säilyttäminen on olennaisen tärkeää yksityisyyden suojaan kohdistuvien riskien minimoimiseksi. Rajoittamalla tietojen keräämistä tiukkojen vaatimusten perusteella organisaatiot vähentävät tietosuojaloukkausten ja henkilötietojen luvattoman käytön todennäköisyyttä ja suojaavat siten yksilöiden yksityisyyttä.

Security

Click cards to flip ↻

Transparency

Click cards to flip ↻

Access and correction

Click cards to flip ↻

Accountability

Click cards to flip ↻

Tietosuojan tärkeimmät seikat

Ongelman määrittely ja liiketoiminnan ymmärtäminen

Huomioon otettavat eettiset periaatteet - Turvallisuus

Consent

Purpose limitation

Data minimization

Tietoturvan varmistaminen on ensiarvoisen tärkeää yksilöiden yksityisyyden suojaamiseksi. Vankkojen turvatoimenpiteiden, kuten salauksen, pääsynvalvonnan ja säännöllisten tietoturvatarkastusten, käyttöönotto auttaa estämään luvattoman pääsyn, tietoturvaloukkaukset ja tietovuodot, mikä varmistaa tietojen luottamuksellisuuden ja eheyden.

Transparency

Click cards to flip ↻

Access and correction

Click cards to flip ↻

Accountability

Click cards to flip ↻

Tietosuojan tärkeimmät seikat

Ongelman määrittely ja liiketoiminnan ymmärtäminen

Huomioon otettavat eettiset periaatteet | Läpinäkyvyys

Consent

Purpose limitation

Data minimization

Security

Selkeä viestintä tietojen käytöstä on olennaisen tärkeää luottamuksen ja vastuullisuuden edistämiseksi. Ollessaan avoimia tietojen käsittelykäytännöistään organisaatiot antavat yksilöille mahdollisuuden ymmärtää, miten heidän tietojaan käytetään, ja tehdä tietoisia valintoja tietojensa jakamisesta.

Access and correction

Click cards to flip ↻

Accountability

Click cards to flip ↻

Tietosuojan tärkeimmät seikat

Ongelman määrittely ja liiketoiminnan ymmärtäminen

Huomioon otettavat eettiset periaatteet | Pääsy ja oikaisu

Consent

Purpose limitation

Data minimization

Security

Transparency

Yksityisyydensuojan perusta on se, että yksilöt voivat käyttää ja korjata omia tietojaan. Antamalla yksilöille mahdollisuuden tarkistaa ja päivittää tietojaan organisaatiot antavat heille mahdollisuuden ylläpitää tietojensa paikkansapitävyyttä ja täydellisyyttä, mikä parantaa yksityisyydensuojaa ja varmistaa tietojen paikkansapitävyyden.

Accountability

Click cards to flip ↻

Tietosuojaan tärkeimmät seikat

Ongelman määrittely ja liiketoiminnan ymmärtäminen

Huomioon otettavat eettiset periaatteet | Vastuullisuus

Consent

Purpose limitation

Data minimization

Security

Transparency

Access and correction

Tietosuojalakien noudattaminen ja vastuullisuus tietojen suhteen ovat olennaisia luottamuksen ja uskottavuuden rakentamisessa. Säännösten noudattaminen, tietosuojakäytäntöjen toteuttaminen ja läpinäkyvien tietokäytäntöjen ylläpitäminen vahvistavat vastuullisuutta ja luottamusta.

Tietosuojan tärkeimmät seikat

Mitä on käytettävyys?

Käytettävyys tarkoittaa sitä, kuinka helposti ja tehokkaasti tehtävät voidaan suorittaa tai kokemuksia parantaa teknologian tai muiden apuvälineiden avulla. Se kattaa toiminnan vaivannäön, ajan ja monimutkaisuuden vähentämisen, mikä lopulta johtaa yksilöiden mukavampaan ja sujuvampaan kokemukseen.

Käytettävyys tekoälyn alalla tarkoittaa teknologian saumatonta integrointia tehtävien virtaviivaistamiseksi ja tehokkuuden parantamiseksi. Tekoälyteknologiat hyödyntävät algoritmeja ja koneoppimista prosessien automatisointiin, manuaalisen työn vähentämiseen ja kokemusten räätälöintiin yksilöllisten mieltymysten mukaan. Analysoimalla valtavia määriä dataa ja oppimalla malleista tekoälyjärjestelmät optimoivat työnkulkuja, säästävät aikaa ja resursseja ja tuottavat parempia tuloksia.

Tietosuoja ja tärkeimmät seikat

Mitä on käytettävyys?

Terveystieteiden tutkimus

Rahoitus

Arkielämä

Terveystieteiden tutkimuksessa tekoäly mahdollistaa potilashoidon automatisoidun diagnostiikan avulla. Tekoälyalgoritmit analysoivat lääketieteellisiä tietoja, kuten kuvantamistutkimuksia ja potilastietoja, auttaakseen terveystieteiden ammattilaisia diagnosoimaan sairauksia tarkasti ja nopeasti. Tunnistamalla nopeasti mallit ja poikkeamat tekoälypohjaiset diagnoosityökalut nopeuttavat diagnoosiprosessia, mahdollistavat oikea-aikaiset toimenpiteet ja parantavat potilaiden hoitotuloksia.



IMAGE SOURCE | Generated by DALL-E

Tietosuojan tärkeimmät seikat

Mitä on käytettävyys?

Terveystieteidenhuolto

Rahoitus

Arkielämä

Rahoitusallalla tekoälypohjainen sijoitusneuvonta tarjoaa yksilöllisiä suosituksia, jotka on räätälöity kunkin asiakkaan taloudellisiin tavoitteisiin ja riskiprofiiliin. Tekoälyalgoritmit analysoivat markkinatrendejä, talousindikaattoreita ja historiallisia tietoja, jotta sijoittajat saavat tietoa sijoitusmahdollisuuksista ja riskitekijöistä. Tekoälyn avulla sijoittajat voivat tehdä tietoon perustuvia päätöksiä, optimoida salkustrategioita ja saavuttaa taloudelliset tavoitteensa tehokkaammin.



IMAGE SOURCE | Generated by DALL-E

Tietosuojan tärkeimmät seikat

Mitä on käytettävyys?

Terveystieteiden tutkimuskeskus

Rahoitus

Arkielämä

Älykkäät kodinkoneet ovat esimerkki käytettävyydestä jokapäiväisessä elämässä, sillä ne parantavat mukavuutta, turvallisuutta ja tehokkuutta. Tekoälyllä toimivat laitteet, kuten älykkäät termostaatit, valaistusjärjestelmät ja virtuaaliassistentit, automatisoivat kotitaloustöitä ja mukautuvat käyttäjän mieltymyksiin. Käyttäjät voivat äänikomennoilla tai automaattisilla aikatauluilla hallita kotinsa ympäristöä vaivattomasti, mikä maksimoi käytettävyyden ja parantaa elämänlaatua.



IMAGE SOURCE | Generated by DALL-E

Tietosuojan tärkeimmät seikat

Mitä on käytettävyys?

Tekoälyteknologioiden mahdollistama käytettävyys kattaa automaation, personoinnin ja tehokkuuden saumattoman integroinnin eri aloilla. Terveystieteiden ja rahoitusalan jokapäiväiseen elämään tekoälypohjaiset ratkaisut optimoivat prosesseja, tehostavat päätöksentekoa ja rikastuttavat kokemuksia, mikä lopulta parantaa tuottavuutta ja yleistä hyvinvointia.

Tietosuojan tärkeimmät seikat

Hypoteettinen skenaario Terveysseurantasovellus

- **Tausta:** Harkitset uuden terveysseurantasovelluksen, HealthMaten, hankkimista. Tämä sovellus tarjoaa henkilökohtaisia kunto- ja ruokavalio-ohjelmia analysoimalla päivittäistä aktiivisuuttasi, ruokavaliotasi ja terveystietojasi.
- **Skenaariohaaste:** HealthMate voi synkronoida tiedot sosiaalisen median tileihisi kerätäkseen lisää elämäntapatietoja, joiden avulla se voi parantaa palvelunsa henkilökohtaisuutta ja jakaa tietoja kumppaneille, jotka voivat lähettää sinulle terveystavoitteisiisi perustuvia kohdennettuja mainoksia.
- **Pohdittavaa:**
 - Hyväksyisitkö palvelun henkilökohtaisuuden parantamisen, vaikka tietosi saattaisivat päätyä kohdennettuun mainontaan?
 - Miten arvioisit räätälöidyn terveystavoitteiden hyödyt verrattuna tietojen jakamisen riskeihin?

YKSITYISYYDEN JA KÄYTETTÄVYYDEN VUOROVAIKUTUS



IMAGE SOURCE | Generated by DALL-E

Yksityisyyden ja käytettävyyden vuorovaikutus

Yksityisyyden ja käytettävyyden välinen kompromissi	+
Eettiset ongelmat	+
Tietosuojaa ja käytettävyyttä koskevien päätösten vaikutukset todellisessa elämässä	+

Yksityisyyden ja käytettävyyden vuorovaikutus

Yksityisyyden ja käytettävyyden vuorovaikutus

Yksityisyyden ja käytettävyyden tasapainottaminen edellyttää näiden kahden tekijän välisten kompromissien löytämistä. Yksityisyys edellyttää usein tietojen keräämisen ja käytön rajoituksia, jotka voivat haitata kätevien palvelujen saumatonta toimittamista. Toisaalta käytettävyyden asettaminen etusijalle voi merkitä yksityisyyden uhraamista, kun henkilötietoihin annetaan laajempi pääsy.

Eettiset ongelmat

+

Tietosuoja ja käytettävyyttä koskevien päätösten vaikutukset todellisessa elämässä

+

Yksityisyyden ja käytettävyyden vuorovaikutus

Yksityisyyden ja käytettävyyden vuorovaikutus

+

-

Eettiset ongelmat

Yksityisyyden ja käytettävyyden välinen vuorovaikutus herättää eettisiä ongelmia, joihin on puututtava. Eettisiin näkökohtiin kuuluu sen määrittäminen, missä määrin yksilöt ovat valmiita tinkimään yksityisyydestään käytettävyyden vuoksi, sekä teknologia-alan yritysten tiedonkeruu- ja käyttötapojen eettisten vaikutusten arviointi.

Tietosuojaa ja käytettävyyttä koskevien päätösten vaikutukset todellisessa elämässä

+

Yksityisyyden ja käytettävyyden vuorovaikutus

Yksityisyyden ja käytettävyyden vuorovaikutus

+

Eettiset ongelmat

+

-

Tietosuoja ja käytettävyyttä koskevien päätösten vaikutukset todellisessa elämässä

Yksilöiden ja organisaatioiden tekemät valinnat yksityisyyden ja käytettävyyden välillä vaikuttavat todelliseen elämään. Käytettävyyden valitseminen yksityisyyden sijaan voi johtaa tietoturvaloukkauksiin, identiteettivarkauksiin tai autonomian menetykseen. Päinvastoin, yksityisyyden asettaminen käytettävyyden edelle voi johtaa henkilökohtaisten palvelujen saatavuuden heikkenemiseen tai haitata teknologian kehitystä, joka perustuu tietojen keräämiseen.

Yksityisyyden ja käytettävyyden vuorovaikutus

Yksityisyyden ja käytettävyyden tasapainottaminen edellyttää huolellista harkintaa kompromisseista ja näiden päätösten eettisistä vaikutuksista. Ymmärtämällä yksityisyyden ja käytettävyyden välisen vuorovaikutuksen yksilöt ja organisaatiot voivat tehdä tietoon perustuvia valintoja, joissa molemmat arvot ovat etusijalla ja mahdolliset riskit ja eettiset huolenaiheet minimoidaan.

TIETOSUOJAN JA KÄYTETTÄVYYDEN TÄRKEYS



IMAGE SOURCE | Generated by DALL-E

Yksityisyyden ja käytettävyyden merkitys

Käyttäjien luottamuksen ja teknologian käyttöönoton parantaminen	+
Tekoälyn käyttöönoton oikeudelliset ja eettiset näkökohdat	+
Vaikutus yhteiskunnallisiin normeihin ja yksilöiden käyttäytymiseen	+

Yksityisyyden ja käytettävyyden merkitys

Käyttäjien luottamuksen ja teknologian käyttöönoton parantaminen

Tietosuojan ja käytettävyyden priorisointi tekoälyteknologioissa on ratkaisevan tärkeää käyttäjien luottamuksen vahvistamiseksi ja tekoälyn yleistymisen edistämiseksi. Kun käyttäjät kokevat, että heidän yksityisyyttään kunnioitetaan ja käytettävyyttä priorisoidaan, he ovat todennäköisemmin valmiita ottamaan tekoälyratkaisut käyttöön. Tarjoamalla käteviä kokemuksia, joissa myös tietosuoja on etusijalla, tekoälyjärjestelmät voivat rakentaa luottamusta käyttäjien keskuudessa, mikä lisää tekoälyn käyttöönottoa ja parantaa käyttökokemusta.

Tekoälyn käyttöönoton oikeudelliset ja eettiset näkökohdat

Vaikutus yhteiskunnallisiin normeihin ja yksilöiden käyttäytymiseen

Yksityisyyden ja käytettävyyden merkitys

Käyttäjien luottamuksen ja teknologian käyttöönoton parantaminen

+

Tekoälyn käyttöönoton oikeudelliset ja eettiset näkökohdat

Oikeudellisten ja eettisten vaikutusten huomioon ottaminen on ensiarvoisen tärkeää tekoälyteknologioita käyttöön otettaessa. Yleinen tietosuojalaki (GDPR) ja muut säännökset asettavat tiukat ohjeet tietosuojalle ja tietojen suojaamiselle varmistuen, että yksilöiden oikeuksia kunnioitetaan. Eettiset viitekehykset ohjaavat tekoälyn kehittämistä vastuullisen ja eettisen tietojen käytön edistämiseksi. Noudattamalla näitä säännöksiä ja viitekehyksiä organisaatiot voivat ottaa tekoälyteknologioita käyttöön tavalla, joka varmistaa tietosuojan ja tietojen eettisen käytön sekä edistää käyttäjien ja sidosryhmien luottamusta.

-

Vaikutus yhteiskunnallisiin normeihin ja yksilöiden käyttäytymiseen

+

Yksityisyyden ja käytettävyyden merkitys

Käyttäjien luottamuksen ja teknologian käyttöönoton parantaminen

+

Tekoälyn käyttöönoton oikeudelliset ja eettiset näkökohdat

+

Vaikutus yhteiskunnallisiin normeihin ja yksilöiden käyttäytymiseen

-

Tekoälyn tapa käsitellä yksityisyyttä ja käytettävyyttä voi vaikuttaa merkittävästi yhteiskunnallisiin normeihin ja yksilöiden käyttäytymiseen. Tekoäly voi muokata yksityisyyttä koskevia odotuksia ja mieltymyksiä vaikuttamalla siihen, miten yksilöt kokevat teknologian ja ovat vuorovaikutuksessa sen kanssa. Lisäksi kätevät tekoälyratkaisut voivat vaikuttaa päivittäisiin rutiineihin ja päätöksentekoprosesseihin tarjoamalla yksilöllisiä kokemuksia, jotka virtaviivaistavat tehtäviä ja parantavat tehokkuutta. Näiden yhteiskunnallisten ja yksilöllisten vaikutusten ymmärtäminen on olennaisen tärkeää, jotta voidaan kehittää tekoälyteknologioita, jotka vastaavat käyttäjien tarpeita ja odotuksia ja kunnioittavat heidän yksityisyydensuojaansa.

Yksityisyyden ja käytettävyyden merkitys

Yhteenvetona voidaan todeta, että tekoälyn käytettävyyden ja yksityisyyden suojaamisen asettaminen etusijalle on ratkaisevan tärkeää käyttäjien luottamuksen rakentamiseksi, GDPR:n kaltaisten säännösten noudattamiseksi ja yhteiskunnallisten normien muokkaamiseksi.

Tasapainottamalla nämä näkökohdat voimme luoda tekoälyjärjestelmiä, jotka parantavat käyttökokemusta ja vaikuttavat myönteisesti yhteiskuntaan.

TIETOSUOJAN JA KÄYTETTÄVYYDEN RISKIT JA EDUT



IMAGE SOURCE | Generated by DALL-E

Tietosuojan ja käytettävyyden riskit ja edut

Mahdolliset riskit	Mahdolliset edut	Riskien vähentäminen
Tietoturvaloukkaukset: Tekoälyjärjestelmät käsittelevät usein valtavia määriä arkaluonteisia tietoja, mikä tekee niistä alttiita tietoturvaloukkauksille. Luvaton pääsy henkilötietoihin voi johtaa identiteettivarkauksiin, taloudellisiin menetyksiin ja maineen vahingoittumiseen. Yksityisyyden menetys: Tekoälyteknologiat voivat kerätä ja analysoida henkilötietoja ilman yksilöiden suostumusta tai tietämystä, mikä vaarantaa heidän yksityisyydensuojansa. Yksityisyyden heikentyminen voi johtaa epäluottamukseen tekoälyjärjestelmiä kohtaan ja huoleen tietojen väärinkäytöstä. Vinoumat tekoälyalgoritmeissa: Tekoälyalgoritmit voivat vahvistaa koulutustiedoissa esiintyviä vinoumia, mikä johtaa syrjiviin tuloksiin. Vinoutuneet tekoälyalgoritmit voivat johtaa epäoikeudenmukaiseen kohteluun tai päätöksentekoon, mikä pahentaa olemassa olevia yhteiskunnallisia eriarvoisuuksia.		

Tietosuojan ja käytettävyyden riskit ja edut

Mahdolliset riskit

Mahdolliset edut

Riskien vähentäminen

Tehokkuuden parantaminen: Tekoäly virtaviivaistaa prosesseja ja automatisoi tehtäviä, mikä parantaa tehokkuutta ja tuottavuutta. Tekoäly hoitaa toistuvat tehtävät, jolloin työntekijät voivat keskittyä arvokkaampiin tehtäviin.

Paremmat datapohjaiset päätökset: Tekoälyalgoritmit analysoivat valtavia määriä dataa paljastaakseen oivalluksia ja malleja, joiden avulla organisaatiot voivat tehdä paremmin perusteltuja päätöksiä. Tekoälyn avulla saadut oivallukset voivat optimoida toimintoja, parantaa asiakaskokemusta ja vauhdittaa innovaatioita.

Parempi käyttökokemus: Tekoälyn avulla käyttökokemusta voidaan parantaa tarjoamalla räätälöityjä suosituksia ja palveluita. Tekoäly parantaa käyttäjien tyytyväisyyttä ja sitoutumista esimerkiksi tarjoamalla henkilökohtaisia tuotesuosituksia tai ennakoivaa huoltoa tuotannossa.

Tietosuojan ja käytettävyyden riskit ja edut

Mahdolliset riskit	Mahdolliset edut	Riskien vähentäminen
Toteuta vankat turvatoimet: organisaatioiden tulisi toteuttaa vankat turvatoimet suojautuakseen tietomurroilta ja luvattomalta pääsylvä. Tähän kuuluvat salaus, pääsynvalvonta ja säännölliset tietoturvatarkastukset. Varmista läpinäkyvyys ja vastuullisuus: läpinäkyvyys ja vastuullisuus ovat olennaisia tekoälyjärjestelmiin luottamuksen rakentamiseksi. Organisaatioiden tulisi olla avoimia tekoälyteknologioiden käytöstä ja varmistaa vastuuvollisuus toiminnastaan. Aseta eettiset näkökohdat etusijalle: eettisten näkökohtien tulisi ohjata tekoälyn kehittämistä ja käyttöönottoa. Organisaatioiden tulisi asettaa etusijalle tekoälyjärjestelmien oikeudenmukaisuus, läpinäkyvyys ja vastuullisuus vinoumien vähentämiseksi ja tietojen eettisen käytön varmistamiseksi.		

Tietosuojan ja käytettävyyden riskit ja edut

Ottamalla käyttöön ennakoivaa riskienhallintaa ja vastuullisia tekoälyn käyttöönottoikäytäntöjä organisaatiot voivat maksimoida tekoälyteknologioiden hyödyt ja minimoida mahdolliset haitat yksilöille ja yhteiskunnalle.

Tapaustutkimus: Tekoäly valvonnassa



IMAGE SOURCE | Generated by DALL-E

Tapaustutkimus: Tekoäly valvonnassa



IMAGE SOURCE | Generated by DALL-E

Skenaario

Vilkaassa kaupungissa paikalliset viranomaiset ottavat käyttöön tekoälypohjaisia valvontajärjestelmiä yleisen turvallisuuden parantamiseksi. Järjestelmät hyödyntävät kehittyneitä teknologioita, kuten kasvojentunnistusta, käyttäytymisen analysointia ja esineiden tunnistusta, julkisten tilojen valvomiseksi, potentiaalisten uhkien tunnistamiseksi ja hätätilanteisiin reagoimiseksi reaaliajassa.

Tapaustutkimus: Tekoäly valvonnassa

Turvallisuuden parantaminen vs. tietosuoja-rikkomukset

Turvallisuuden parantaminen

Tekoälypohjaiset valvontajärjestelmät tehostavat turvallisuustoimenpiteitä antamalla lainvalvontaviranomaisille mahdollisuuden havaita nopeasti epäilyttävät toimet tai mahdolliset turvallisuusuhkat ja reagoida niihin.

Kasvontunnistustekniikka auttaa tunnistamaan tarkkailulistoilla olevia tai kadonneiksi ilmoitettuja henkilöitä, mikä helpottaa oikea-aikaista puuttumista ja parantaa yleistä turvallisuutta

Tietosuoja-rikkomukset

Turvallisuusetuista huolimatta tekoälyvalvontaan liittyy huolenaiheita mahdollisten yksityisyyden loukkausten vuoksi. Jatkuva seuranta ja tiedonkeruu julkisilla paikoilla herättävät kysymyksiä yksilön oikeudesta yksityisyyteen ja vapauteen jatkuvasta valvonnasta.

On olemassa virheellisen tunnistamisen ja väärin hälytysten riski, mikä voi johtaa syyttömien henkilöiden väärin perusteisiin syytöksiin ja yksityisyyden loukkauksiin, jos järjestelmä merkitsee heidät virheellisesti.

Tapaustutkimus: Tekoäly valvonnassa

Turvallisuuden parantaminen vs. tietosuojarikkomukset

Lisätietoja harkitun tekoälyn käyttöönoton tärkeydestä

Selkeät toimintaperiaatteet ja säännöt	+
Tietojen eettinen käyttö	+
Algoritmien läpinäkyvyys ja vastuullisuus	+
Yleisön osallistuminen ja valvonta	+

Tapaustutkimus: Tekoäly valvonnassa

Turvallisuuden parantaminen vs. tietosuojarikkomukset

Lisätietoja harkitun tekoälyn käyttöönoton tärkeydestä

Selkeät toimintaperiaatteet ja säännöt	-
Harkittu tekoälyn käyttöönotto edellyttää selkeiden käytäntöjen ja sääntöjen laatimista valvontateknologian käytöstä, jotta varmistetaan läpinäkyvyys, vastuullisuus ja tietosuojalakien noudattaminen.	
Ethical use of data	+
Algorithmic transparency and accountability	+
Public engagement and oversight	+

Tapaustutkimus: Tekoäly valvonnassa

Turvallisuuden parantaminen vs. tietosuojarikkomukset

Clear policies and regulations	+
Tietojen eettinen käyttö Organisaatioiden on asetettava etusijalle valvontajärjestelmien avulla kerättyjen tietojen eettinen käyttö, kunnioittamalla yksilöiden oikeutta yksityisyyteen ja minimoimalla yksityisyyden loukkausten tai henkilötietojen väärinkäytön riski.	-
Algorithmic transparency and accountability	+
Public engagement and oversight	+

Tapaustutkimus: Tekoäly valvonnassa

Turvallisuuden parantaminen vs. tietosuoja-rikkomukset

Clear policies and regulations	+
Ethical use of data	+
Algoritmien läpinäkyvyys ja vastuullisuus Läpinäkyvien tekoälyalgoritmien ja vastuuvollisuuden mekanismien käyttöönotto varmistaa, että valvontajärjestelmät ovat oikeudenmukaisia, tarkkoja ja vastuullisia toimistaan, mikä vähentää yksityisyyden loukkauksiin johtavien vinoumien tai virheiden riskiä.	-
Public engagement and oversight	+

Tapaustutkimus: Tekoäly valvonnassa

Turvallisuuden parantaminen vs. tietosuojarikkomukset

Clear policies and regulations	+
Ethical use of data	+
Algorithmic transparency and accountability	+
Yleisön osallistuminen ja valvonta Yleisön osallistaminen tekoälyn valvontaa koskeviin keskusteluihin ja sidosryhmien osallistaminen päätöksentekoon edistää avoimuutta, luottamusta ja vastuullisuutta sekä vastuullista valvontateknologian käyttöönottoa ja käyttöä.	-

Tapaustutkimus: Tekoäly valvonnassa

Yhteenvetona voidaan todeta, että tekoälyn käyttö valvonnassa korostaa tarvetta harkita tekoälyn käyttöönottoa huolellisesti ja tasapainottaa turvallisuuden parantaminen ja yksityisyyden suoja.

Asettamalla etusijalle eettiset periaatteet, avoimuuden ja vastuuvollisuuden organisaatiot voivat ottaa käyttöön valvontajärjestelmiä, jotka parantavat turvallisuutta ja samalla kunnioittavat yksilöiden yksityisyyden suojaa ja vahvistavat kansalaisten luottamusta.

JOHTOPÄÄTÖS



IMAGE SOURCE | Generated by DALL-E

JOHTOPÄÄTÖS

1. Ymmärtää tekoälyjärjestelmien yksityisyyden ja käytettävyyden monimutkaisen suhteen ja tunnistaa niiden keskeinen rooli vastuullisessa teknologian integroinnissa.
2. Tutkia tietosuojan keskeisiä näkökohtia ja niiden vaikutuksia, mukaan lukien suostumus, turvallisuus ja eettiset tietojen käsittelykäytännöt.
3. Analysoida yksityisyyden ja käytettävyyden risteyskohdat tekoälysovelluksissa ja arvioida sekä potentiaalisia riskejä, kuten tietoturvaloukkauksia ja vinoumia, että etuja, kuten tehokkuuden parantumista ja käyttäjäkokemuksen parantumista.
4. Korostaa harkitun tekoälyn käyttöönoton merkitystä, kuten todellisessa tapausesimerkissä tekoälyn käytöstä valvonnassa, turvallisuuden parantamisen ja yksityisyyden suojan välisen tasapainon saavuttamiseksi, mikä lopulta edistää luottamusta, innovaatioita ja yhteiskunnan hyvinvointia.

JOHTOPÄÄTÖS

”Digitaalisella aikakaudella, erityisesti tekoälyn yleistyessä, yksityisyyden suojaaminen tarkoittaa näiden kolmen keskeisen näkökohdan huomioon ottamista. Tekoälyteknologioiden integroitua yhä enemmän elämäämme, yksityisyyden suojaaminen on yhä suurempi haaste, joka edellyttää sekä oikeudellisten viitekehysten että teknisten toimenpiteiden valppaista soveltamista.”

KIITOS



Universitat
de les Illes Balears



helixconnect



**Euroopan unionin
osarahoittama**

Euroopan unionin rahoittama. Esitetyt näkemykset ja mielipiteet ovat ainoastaan tämän tekstin laatijoiden näkemyksiä eivätkä välttämättä vastaa Euroopan unionin tai Euroopan koulutuksen ja kulttuurin toimeenpanovirasto (EACEA) kantaa. Euroopan unioni ja EACEA eivät ole vastuussa niistä.

2022-1-ES01-KA220-HED-000085257