

4 . N O D A R B Ī B A

Mākslīgais intelekts un likums

Juridiskais regulējums, autortiesības un atbildība bibliotēku kontekstā

 90 min | Jebkuram interesentam

Juridiskā vide

Mākslīgā intelekta ieviešana bibliotēkās rada aktuālus juridiski risināmus jautājumus:

© Autortiesības

Kādi ir MI apmācības datu un ar MI palīdzību veidota satura radīšanas riski?

Datu aizsardzība

Kā datu regula tiek piemērota, kad mākslīgais intelekts apstrādā lietotāju datus, vaicājumus vai profilus?

ES Mākslīgā intelekta akts

Pasaulē pirmā visaptverošā MI regula: riska klasifikācija, ieviesēja pienākumi un izpilde.

Atbildība

Kas notiek, ja mākslīgais intelekts pieļauj kļūdas? Kurš ir atbildīgs – bibliotēka vai pakalpojuma sniedzējs?

Autortiesības un MI

D A T I

Mākslīgā intelekta modeļi tiek apmācīti, izmantojot liela apjoma datu kopas, kas bieži ietver autortiesībām pakļautu materiālu. Trīs galvenie juridiskie jautājumi bibliotēkām:

1

Vai mākslīgā intelekta izstrādātājiem ir nepieciešama atļauja, lai apmācībai izmantotu ar autortiesībām aizsargātu saturu?

2

Vai modeļu apmācība, izmantojot ar autortiesībām aizsargātu materiālu, ir autortiesību pārkāpums?

3

Kā ES, ASV un Apvienotās Karalistes regulējums atšķiras attiecībā uz teksta un datu ieguves (TDM) izņēmumiem?

ES autortiesību direktīva (2019/790)

Pētniecības organizācijām un kultūras mantojuma institūcijām ieviests teksta un datu ieguves izņēmums. Bibliotēkas var to izmantot, taču nav skaidrs, vai šis izņēmums attiecas arī uz komerciālu MI apmācību.

Autortiesības un MI

KAM PIEDER MI RADĪTS SATURS

04

Lielākajā daļā jurisdikciju

Autortiesībām ir nepieciešams reāls autors. Mākslīgā intelekta ģenerēts saturs bez jēgpilnas cilvēka radošas iesaistes var nebūt aizsargāts ar autortiesībām.

Pakalpojuma sniedzēja noteikumi atšķiras

Pakalpojuma lietošanas noteikumi būtiski atšķiras – MI ģenerētais saturs var piederēt lietotājam, pakalpojuma sniedzējam vai arī nonākt publiskajā domēnā.

Praktiski apsvērumi bibliotēkām

Rūpīgi pārskatiet MI pakalpojuma sniedzēju līgumus, lai izprastu mākslīgā intelekta ģenerēta satura autortiesības, īpaši, ja saturs tiks publicēts vai kopīgots (piemēram, ierakstu katalogi, meklēšanas palīg līdzekļi, lietotājiem paredzēts teksts).

Datu aizsardzība

Likumīgais pamats

Bibliotēkām jāidentificē atbilstošs tiesiskais pamats personas datu apstrādei ar MI palīdzību: leģitīmās intereses, datu subjekta piekrišana vai uzdevuma veikšana sabiedrības interesēs.

Datu minimizēšana

Mākslīgā intelekta rīkiem nevajadzētu apkopot vai apstrādāt vairāk personas datu, nekā nepieciešams norādītajam mērķim.

Automatizēti lēmumi

Datu aizsardzības regula ierobežo tikai automatizētus lēmumus.

Novērtējums par ietekmi uz datu aizsardzību (NIDA)

Datu aizsardzības ietekmes novērtējums var būt nepieciešams, ja MI sistēmā tiek apstrādāti personas dati un šāda apstrāde var radīt augstu risku fizisku personu tiesībām un brīvībām.



Bibliotēka = datu pārzinis. Mākslīgā intelekta pakalpojuma sniedzējs = datu apstrādātājs. Obligāti jānoslēdz datu regulai atbilstošs datu apstrādes līgums (DPA).

KĀPĒC MI AKTS?





Dutch Rutte government resigns over child welfare fraud scandal



Dutch PM Mark Rutte said in January 2021 the decision to resign was "unavoidable"



You're a single mother with three children aged eight to 11. You hit rock-bottom financially and think what now? My children and I sometimes had to go to bed without food

Dulce Gonçalves Tavares

Told in 2013 she had to pay back €125,000



Last month, Prime Minister of the Netherlands Mark Rutte—along with his entire cabinet—resigned after a year and a half of investigations revealed that since 2013, 26,000 innocent families were wrongly accused of social benefits fraud partially due to a discriminatory algorithm.

Audit of 9 government algorithms finds 6 do not meet basic requirements

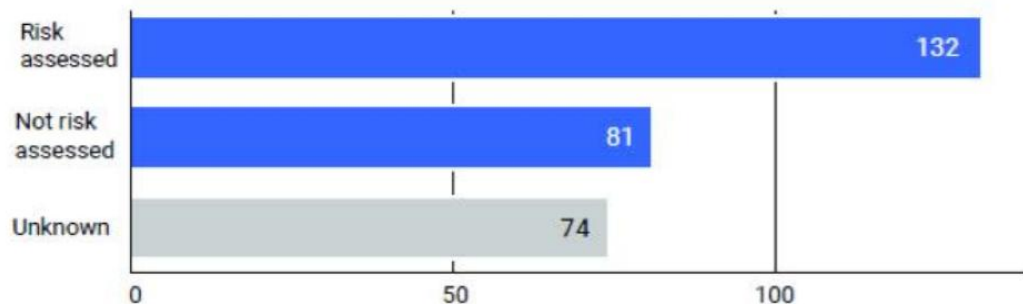
News item | 18-05-2022 | 10:45

Responsible use of algorithms by government agencies is possible but not always the case in practice. The Netherlands Court of Audit found that 3 out of 9 algorithms it audited met all the basic requirements, the other 6 did not and exposed the government to various risks: from inadequate control over the algorithm's performance and impact to bias, data leaks and unauthorised access.



Figure 14 *Risk assessment of AI systems*

Not all AI systems underwent a risk assessment



This figure presents information on only the 287 AI systems currently under development or in use.

Pasaulē pirmais spēkā esošais visaptverošs MI tiesiskais regulējums, kas balstās uz MI radītu risku novērtējumu.

NEPIEŅEMAMS RISKS — Aizliegtas darbības. Pilnībā aizliegts.

AUGSTS RISKS — Stingras prasības, cilvēka uzraudzība, nepieciešami ietekmes novērtējumi.

IEROBEŽOTS RISKS — Prasības pārredzamībai : informējiet lietotājus par MI izmantošanu.

MINIMĀLS RISKS — Nav īpašu saistību; ieteicams ievērot brīvprātību.

Nepieņemams risks

- Maldinošas vai manipulatīvas metodes
- Personiskās ievainojamības izmantošana
- Biometriskās kategorizācijas sistēmas, kas izmanto sensitīvus datus
- Sociālā vērtēšana
- Personas noziedzīgu nodarījumu riska novērtēšana
- Sejas atpazīšanas datubāzu apkopošana
- Emociju atpazīšana darba vietās vai izglītības iestādēs
- Attālināta biometriskā identifikācija (RBI) "reāllaikā" publiski pieejamās vietās

Augsts risks

- Biometriskās sistēmas, kas nav aizliegtas
- Kritiskā infrastruktūra
- Izglītība un profesionālā apmācība
- Nodarbinātība, darbinieku pārvaldība un piekļuve pašnodarbinātībai
- Piekļuve būtiskiem sabiedriskajiem un privātajiem pakalpojumiem un to izmantošana
- Tiesībaizsardzība
- Migrācijas, patvēruma un robežkontroles pārvaldība
- Tieslietu administrēšana un demokrātiskie procesi

Augsts risks

Pakalpojumu sniedzējiem ir jāizpilda šādas prasības:

- Risku pārvaldības sistēma
- Datu pārvaldība
- Tehniskā dokumentācija
- Uzskaitē
- Instrukciju rokasgrāmata
- Nodrošināt cilvēka veiktu uzraudzību

Ierobežots risks

- Obligāta pārredzamība
- Piemēri: dziļviltojumi

Minimāls risks

- Neregulēti
- Piemēri: surogātpasta filtri, videospēles ar MI elementiem

ES Mākslīgā intelekta akts — piemēri

Kurā risku klasifikācijas kategorijā ietilpst bibliotēku MI rīki?

MI rīks un pielietojums	Riska līmenis	Prasības
Klientu sociālā vērtēšana/uzraudzība	 Nepieņemams	Aizliegts izvietot
Klientu profilēšana/uzvedības prognozēšana	 Augsts risks	Cilvēka uzraudzība + incidentu reģistrēšana ir obligāta
Mākslīgā intelekta tērēšanas robots uzzīņu jautājumiem	 Ierobežots risks	Jāatklāj, ka lietotāji mijiedarbojas ar mākslīgo intelektu
Mākslīgā intelekta ģenerēta satura veidošanas rīki	 Ierobežots risks	Skaidri apzīmējiet rezultātus kā mākslīgā intelekta ģenerētus
Katalogizēšana ar mākslīgā intelekta palīdzību	 Minimāls risks	Nav īpašu saistību, ievērojiet labu praksi

ES Mākslīgā intelekta akts — piemēri

Bibliotēkas, kas izmanto MI rīkus kā gala lietotājas, saskaņā ar MI aktu tiek klasificētas kā MI sistēmu izmantotāji, un tām ir noteikti juridiski pienākumi.

AUGSTA RISKA SISTĒMAS

- Pirms izvietošanas jāveic pamattiesību ietekmes novērtējumu
- Vienmēr nodrošiniet cilvēka uzraudzību
- Informējiet personas, ja tās ietekmē ar mākslīgā intelekta palīdzību pieņemti lēmumi

VISPĀRĒJI MĀKSLĪGĀ INSTRUMENTA RĪKI (piemēram, *ChatGPT*, *Claude*, *Gemini*)

- Izmantojiet tikai paredzētajam mērķim, ko noteicis pakalpojumu sniedzējs
- Neizmantojiet tādos veidos, kas rada riskus, kuri nav aprakstīti dokumentācijā
- Pirms parakstīšanas pieprasiet no piegādātājiem atbilstības dokumentāciju

AR MĀKSLĪGO INTELEKTU ĢENERĒTS SATURS UN SARUNBOTI

- Informējiet lietotājus, ka viņi mijiedarbojas ar mākslīgā intelekta sistēmu
- Skaidri apzīmējiet visus mākslīgā intelekta ģenerētos rezultātus
- Neizmantojiet dziļviltojumus vai ģenerētu saturu bez skaidras informācijas norādīšanas

Atbildība — kad mākslīgais intelekts kļūdās

Mākslīgā intelekta sistēmas var radīt neprecīzus, neobjektīvus vai kaitīgus rezultātus. Bibliotēku kontekstā tas var ietvert:

Nepareizus ierakstus

Nekorekti MI katalogizēšanas rīku ģenerēti bibliogrāfiskie ieraksti vai atsauces.

Neobjektīvus rezultātus

MI balstītas rekomendāciju vai piekļuves sistēmas var radīt neobjektīvus vai diskriminējošus rezultātus.

Privātuma pārkāpumus

Privātuma pārkāpumi, ko izraisa MI ģenerēts saturs, kas atsaucas uz reālām personām.

Dezinformāciju

Dezinformācija, kas tiek sniegta, izmantojot mākslīgā intelekta darbinātus atbilstošus rīkus.

Līgumi ar MI pakalpojumu sniedzējiem ir būtisks aizsardzības mehānisms. Pārlicinieties vai tie satur: zaudējumu atlīdzināšanu, atbildības ierobežojumi, precizitātes garantijas, ziņošana par incidentiem un datu pārnesamība pēc sadarbības izbeigšanas.

Bibliotekāra juridiskais komplekts

Prasmes, ko jūs jau izmantojat avotu izvērtēšanai, ir tieši piemērojamas mākslīgā intelekta tiesību aktiem.

Juridiskā joma	Galvenais jautājums, kas jāuzdod
Autortiesības	Kam pieder rīks? Vai tas tika apmācīts ar materiāliem, kurus aizsargā autortiesības?
Datu aizsardzība	Vai šis rīks apstrādā personas datus? Vai ir nepieciešams novērtējums par ietekmi un datu aizsardzību (NIDA) un datu apstrādes līgums?
ES MI akts	Kādā riska līmenī ietilpst šī sistēma? Kādi ir mūsu pienākumi kā ieviesējiem?
Atbildība	Ja mākslīgais intelekts pieļauj kļūdu vai nodara kaitējumu, kurš uzņemas juridisko atbildību?
Pakalpojumu sniedzēja līgums	Vai līgums attiecas uz atlīdzināšanu, ziņošanu par incidentiem un datu dzēšanas tiesībām?

MI atslēgas vārdu krājums

ES MI akts

Regula (ES) 2024/1689 — pasaulē pirmais visaptverošais MI tiesību akts, kurā mākslīgā intelekta sistēmu un to ieviešanu regulēšanai tiek izmantota uz risku balstīta pieeja.

GPAI modelis

Vispārējas nozīmes mākslīgā intelekta modelis, ko izmanto par produkta pamatu, ievērojot īpašas saistības.

Teksta un datu ieguve

Autortiesību izņēmums, kas ļauj automatizēti analizēt saturu — ar atšķirīgiem nosacījumiem ES, ASV un Apvienotās Karalistes jurisdikcijās.

Ieviesējs

Organizācija (piemēram, bibliotēka), kas savā darbībā izmanto mākslīgā intelekta sistēmu, un tā nav šīs sistēmas nodrošinātāja vai izstrādātāja.

NIDA

Novērtējums par ietekmi uz datu aizsardzību — process pirms tāda mākslīgā intelekta ieviešanas, kas, visticamāk, radīs augstu risku fizisko personu tiesībām.

Atlīdzināšana

Līguma klauzula, kurā viena puse piekrīt segt otras puses juridisko atbildību vai finansiālos zaudējumus.



Aktivitāte

- 1. gadījuma izpēte: Bibliotēka izmanto MI tērzēšanas robotu grāmatu ieteikšanai. Tas nejauši saglabā lasītāju sarunu vēsturi ar viņu personīgajām interesēm un izvēlēm.
- 2. gadījuma izpēte: Drošības nolūkos tiek ierosināts ieviest sejas atpazīšanas sistēmu. Vai mākslīgā intelekta likums to atļauj? Kādi drošības pasākumi ir nepieciešami?
- 3. gadījuma izpēte: Students ģenerē eseju, izmantojot *ChatGPT*. Bibliotēkai tiek lūgts kopīgot studenta meklēšanas vēsturi ar skolu.

Grupā analizējiet savu gadījumu, kas saistīts ar mākslīgo intelektu, datu privātumu un atbilstību tiesību aktiem, lai noteiktu labāko rīcības plānu saskaņā ar likumiem.



Diskusija

Q1

Vai jūsu iestādei ir mākslīgā intelekta pakalpojumu iepirkumu politika? Kas pārskata piegādātāju līgumus, lai nodrošinātu atbilstību tiesību aktiem?

Q2

Vai esat izmantojuši MI rīkus satura (ierakstu, kopsavilkumu, aprakstu) ģenerēšanai? Kam pieder šis saturs?

Q3

Kā jūs izskaidrotu ES Mākslīgā intelekta akta riska klasifikāciju kolēģim, kurš par to nekad nav dzirdējis?

Q4

Kāds juridiskais jautājums par mākslīgo intelektu jūsu bibliotēkā šobrīd šķiet aktuālākais?