Menneskerettigheder & AI

Når offentlige myndigheder anvender AI, forskydes magten fra myndighederne til de private virksomheder, der udvikler og kontrollerer AI-systemerne. Det udfordrer menneskerettigheder som retten til privatliv, databeskyttelse, ligebehandling samt demokratisk deltagelse. Artiklen undersøger med fokus på AI-forordningen fra 2024, hvordan EU-retten søger at imødegå disse udfordringer bl.a. gennem menneskeretlige konsekvensanalyser. Kravet om menneskeretlige konsekvensanalyser er positivt og styrker potentielt borgerens position. Men samtidig flyttes ansvaret for den menneskeretlig afvejning fra lovgiver til de aktører, der anvender teknologien. Dette skaber et paradoks: Mens reguleringen sigter mod at fremme fleksibilitet og innovation, mindskes den demokratiske kontrol med, hvordan borgerens grundlæggende rettigheder beskyttes. Dette skærper kravene til et effektivt tilsyn med reglernes overholdelse og kræver, at de berørte borgere er i stand til at reagere, hvis der ikke sker den nødvendige beskyttelse af deres rettigheder.

1. Introduktion: den menneskeretlige udfordring

RIKKE FRANK JØRGENSEN
Seniorforsker, Institut for Menneskerettigheder,
rfj@humanrights.dk

ANJA MØLLER PEDERSEN
Tenure track adjunkt, JUR – Center for Ret og Sikkerhed, Københavns Universitet,
anja.moeller.pedersen@jur.ku.dk

Den øgede brug af kunstig intelligens (AI) rejser ikke alene teknologiske og økonomiske spørgsmål, men også fundamentale problemstillinger for borgeren og dennes rettigheder i et demokratisk samfund. AI kan bidrage til at frigøre ressourcer i den offentlige forvaltning, men samtidig sætter teknologien borgerens grundlæggende rettigheder – retten til privatliv, databeskyttelse, ligebehandling og demokratisk deltagelse – under pres.

Fra et rettighedsperspektiv er det særligt problematisk, at AI-systemer ofte opererer i det skjulte og dermed kan forstærke den eksisterende asymmetri i viden og magt mellem stat og borger. Borgeren ved sjældent, hvordan AI spiller ind i en konkret afgørelse, og selv når de er klar over, at AI har spillet en rolle, er det næsten umuligt at gennemskue, hvilke kriterier og data den AI-baserede beslutning bygger på. Hertil kommer, at AI aldrig er neutral (Solove, 2025: 24), og selv den mest avancerede algoritme er ikke bedre end de data, hvorpå den er trænet. Dette medfører risiko for fejlagtige konklusioner, bias mv., samtidig med at borgere får sværere ved at kontrollere de afgørelser, der vedrører dem.

Denne asymmetri i viden underminerer retten til effektivt at kunne anfægte en afgørelse, hvilket er en hjørnesten i menneskeretten og retssikkerheden. Når borgeren ikke kan forstå eller kontrollere de mekanismer, der påvirker

deres liv, reduceres deres mulighed for at handle som aktive demokratiske borgere. Konsekvensen er, at AI kan forstærke en allerede eksisterende magtasymmetri: Staten får øget kapacitet til at overvåge, kategorisere og træffe beslutninger om borgeren, mens borgerens indflydelse på disse processer svækkes. Dette kan medføre, at tilliden til de institutioner, der anvender teknologien, undergraves, fordi borgeren oplever en afstand mellem sig selv og beslutningsprocessen – en afstand, der ikke blot er teknologisk, men også demokratisk og menneskeretlig.

Samtidig sker der en magtforskydning fra de offentlige myndigheder, der er underlagt demokratisk kontrol, til de private aktører, der udvikler de AI-løsninger, som myndighederne benytter. Det kan være vanskeligt for den offentlige myndighed, der benytter en AI-løsning, at forklare, hvordan AI indgår i en afgørelse, da systemerne er komplekse og ofte udviklet af private teknologi-virksomheder. Og når vi taler om de helt store og mest udbredte AI-løsninger, vil disse virksomheder ofte være techgiganter, som på grund af deres størrelse og markedsdominans allerede udgør en reel magtfaktor (Bradford, 2020; EU-Domstolen, 2024; Zuboff, 2019).

Techgiganternes magt kommer bl.a. til udtryk, når deres AI-løsninger bliver brugt til at filtrere resultater på søgemaskiner, til at moderere nyheder på sociale medieplatforme og nyhedsmedier, og til at bestemme, hvilke stemmer der henholdsvis løftes og nedtones i den offentlige debat. Fordi deres tjenester er så udbredte, har de største tech-virksomheder fået afgørende indflydelse på "sandheden", herunder den, der skal gøre borgerne i stand til at udøve deres demokratiske rettigheder.

Dette forskyder magten fra dem, der træffer AI-baserede beslutninger til dem, der udvikler og kontrollerer de AI-løsninger, beslutningerne bliver truffet på baggrund af. Uanset om AI-løsningerne er fuldautomatiserede eller alene bruges som beslutningsstøtte. Det betyder, at velfærdsstatens normative fundament baseret på rettigheder som værdighed, lighed og deltagelse i praksis påvirkes af AI-systemers data-drevne logikker.

Det er derfor afgørende, at reguleringen af AI tager udgangspunkt i borgerens perspektiv. Udviklingen og anvendelsen af AI må ske inden for rammer, der sikrer respekt for menneskerettighederne og demokratiets legitimitet. Kun ved at fastholde borgeren som centrum kan vi sikre, at teknologien bliver et redskab til at styrke – og ikke svække – de værdier, vores samfund bygger på.

2. Den menneskeretlige ramme

AI-systemer kan påvirke en bred vifte af grundlæggende rettigheder – fra retten til privatliv og databeskyttelse til ytringsfrihed, ikke-diskrimination og retten til en retfærdig rettergang. Den overordnede menneskeretlige ramme i Europa hviler primært på Den Europæiske Menneskerettighedskonvention (EMRK) (Europarådet, 1950) og EU's Charter om Grundlæggende Rettig-

heder (Den Europæiske Union, 2016). EMRK sikrer bl.a. retten til privatliv og ytringsfrihed, der er centrale i en AI-kontekst, f.eks. i beskyttelsen mod overvågningsteknologier og algoritmisk indholdsmoderation. EU-chartret indeholder tilsvarende rettigheder, og har særlig betydning for den EU-teknologiregulering, der er blevet vedtaget de senere år, da EU-chartret binder EU's institutioner og EU's medlemsstater, når de gennemfører EU-retten, herunder forordningen om kunstig intelligens (AI-forordningen), der er udformet med henvisning til EU's charter (Europa-Parlamentet og Rådet, 2024a).

En grundlæggende udfordring er, at menneskerettigheder primært binder stater, ikke private aktører. Den Europæiske Menneskerettighedsdomstols doktrin om positive forpligtelser udvider statens pligt, så den udover forpligtelsen til ikke at foretage vilkårlige indgreb i individets rettigheder også skal sikre en effektiv beskyttelse af rettigheder i relationer mellem private parter (Koch, 2005). Databeskyttelsesforordningen (Europa-Parlamentet og Rådet, 2016), der pålægger både myndigheder og virksomheder omfattende databeskyttelsesforpligtelser, kan ses som EU-lovgivers realisering af den positive forpligtelse til at sikre retten til beskyttelse af personoplysninger og privatliv (Den Europæiske Menneskerettighedsdomstol, 2008). Hertil kommer EU-Domstolens doktrin om direkte virkning, der betyder, at borgeren under visse betingelser kan støtte direkte ret på EU-chartrets rettigheder, det vil sige uafhængigt af den nationale implementering, der ellers måtte kræves, over for staten (vertikal virkning) og andre private parter (horisontal virkning). EU-Domstolen har anerkendt en sådan direkte virkning i forhold til EU-chartret i relation til forbuddet mod diskrimination (artikel 21) og arbejdsvilkår (artikel 31) (se f.eks. Bauer-sagen; Den Europæiske Unions Domstol, 2018), og forskere peger på, at dette gælder de fleste af EU-chartrets bestemmelser, herunder retten til beskyttelse af personoplysninger i artikel 8 (Frantziou, 2019).

På globalt plan er FN's retningslinjer for erhvervsliv og menneskerettigheder (United Nations Human Rights Council, 2011) den gældende baseline for virksomheders menneskeretlige ansvar, bl.a. gennem krav om menneskeretlige konsekvensanalyser. UNGP er imidlertid – som betegnelsen 'retningslinjer' indikerer – baseret på frivillighed og således ikke juridisk bindende. Hvis vi vil sikre, at både offentlige og private aktører er underlagt klare menneskeretlige forpligtelser i udvikling og brug af AI, kræver det, at de menneskeretlige forpligtelser operationaliseres gennem bindende lovgivning, standarder og håndhævelsesmekanismer. GDPR og AI-forordningen er centrale eksempler på regulering, der søger dette f.eks. gennem krav om obligatoriske vurderinger af, hvorledes databehandling eller højrisiko-AI-systemer påvirker individets grundlæggende rettigheder.

3. EU's tilgang til at regulere AI (og data)

EU har positioneret sig som global frontløber i reguleringen af digitale teknologier og de virksomheder, der udvikler dem, gennem en rettighedsorienteret og risikobaseret tilgang (Jørgensen et al., 2024; De Gregorio & Dunn, 2022). Denne tilgang blev først tydelig med GDPR, der indførte et princip om ansvarlighed og en risiko-baseret tilgang, som nu er videreført i AI-forordningen, der regulerer AI-systemer ud fra deres potentielle skadevirkninger for sundhed, sikkerhed samt individets grundlæggende rettigheder (artikel 1).

GDPR regulerer behandling af personoplysninger, også i forbindelse med AI, med særligt fokus på at begrænse fuldautomatiserede afgørelser med retsvirkning for individet (artikel 22); at sikre gennemsigtighed i algoritmiske processer ved informationspligter og indsigtsrettigheder (artikel 12-15); at sikre ansvarlighedsprincippet ved at pålægge de dataansvarlige at foretage risikovurderinger og dokumentere, at de overholder reglerne (artikel 5(2) og 24(1)), samt foretage konsekvensanalyser for databeskyttelse (DPIA) ved højrisiko-behandling, f.eks. profilering (artikel 35).

Den risikobaserede tilgang er fleksibel for så vidt, at den kræver en vurdering og afvejning af risici og passende foranstaltninger, hvilket har været med til at gøre GDPR til en global standard for databeskyttelse. EU har videreført den risikobaserede tilgang i nyere lovgivning som Digital Services Act (DSA) (Europa-Parlamentet og Rådet, 2022) og AI-forordningen (Europa-Parlamentet) og (Rådet, 2024b). Sidstnævnte går skridtet videre ved at indføre en systematisk risikoklassificering.

AI-forordningen, vedtaget i 2024, er verdens første omfattende AI-regulering og bygger på en gradueret risikomodel, hvor AI-systemer opdeles i fire risikokategorier. 1) Systemer, der er forbudt (uacceptabel risiko), som f.eks. social scoring og manipulerende AI rettet mod sårbare grupper. 2) Systemer, der indebærer en høj risiko for grundlæggende rettigheder, f.eks. systemer til biometrisk identifikation, kreditvurdering, rekruttering og sundhedsdiagnostik. Sådanne højrisiko-systemer kræver bl.a. et risikostyringssystem, teknisk dokumentation, logning, menneskelig overvågning og CE-mærkning. 3) Systemer med begrænset risiko, hvor der alene stilles krav om gennemsigtighed, f.eks. chatbots og deepfakes (skal mærkes som AI-genereret). Og endelig 4) systemer, der vurderes at udgøre en minimal risiko, og hvor der ikke er særlige krav, f.eks. spamfiltre og søgemaskinealgoritmer. Ved overtrædelse af AI-forordningens forpligtelser kan der tildeles bøder på op til €35 mio. eller 7 % af den pågældende virksomheds globale omsætning.

En nyskabelse i AI-forordningen er kravet om konsekvensanalyser for grundlæggende rettigheder (FRIA) for visse brugere af højrisiko-AI, især offentlige myndigheder og private aktører med offentlige funktioner (f.eks. sundhed, uddannelse, kreditvurdering). Konsekvensanalyserne skal identificere de grundlæggende rettigheder, systemet kan påvirke (f.eks. privatliv, ikke-diskrimination, adgang til retfærdig behandling); beskrive brugskontekst, berørte

grupper og risici; samt angive menneskelig overvågning og afhjælpende foranstaltninger. Dette skal rapporteres til tilsynsmyndigheder inden systemet tages i brug.

AI-forordningens konsekvensanalyser minder om de konsekvensanalyser, der følger af GDPR, og de berørte aktører kan derfor bygge oven på og supplere allerede eksisterende databeskyttelsesretlige konsekvensanalyser, men fokusere mere eksplicit på alle de rettigheder, der direkte kan påvirkes af et AI-system. For både GDPR og AI-forordningen gælder, at der er en tæt konceptuel sammenhæng med UNGP, og de to regelsæt kan således siges at operationalisere forpligtelsen til at udøve rettidig omhu (due diligence) for rettigheder i henholdsvis en databehandlings- og AI-kontekst.

4. Rettigheds- og risikoregulering

EU's AI-forordning har skabt en fælles – bindende – juridisk ramme for udvikling og brug af kunstig intelligens i EU. Forordningen bygger som beskrevet ovenfor på en risikobaseret tilgang. I modsætning til GDPR opdeler AI-forordningen AI-systemer i faste risikokategorier, og disse kategorier afgør, om der skal laves en konsekvensanalyse for grundlæggende rettigheder. Hvis et system er omfattet, skal den ansvarlige – uanset om det er en offentlig myndighed eller en privat virksomhed – selv vurdere og håndtere de konkrete risici for individets rettigheder.

Hvordan skal man karakterisere denne form for regulering? Tilgangen minder om den menneskeretlige beskyttelse i EU-chartret og EMRK, fordi den kræver en afvejning af rettigheder og risici ud fra proportionalitetsprincippet. Men AI-forordningens "meta-regulering" adskiller sig fra den forpligtelse, EU-chartret og EMRK pålægger medlemsstaterne ved netop ikke selv at regulere rettighederne – den fastsætter kun en pligt til at håndtere risikoen for rettigheder, altså den pligt, der normalt påhviler lovgiver selv (Gellert, 2020). Tilgangen minder derfor også om risk-management i organisationer i relation til f.eks. informationssikkerhed, men da AI-forordningen fokuserer på at minimere risikoen for individets rettigheder, fremfor risikoen for skade på organisationen, er det heller ikke helt det, der er på spil.

Fra et menneskeretligt perspektiv, er det afgørende punkt, at EU-lovgiver har ladet det være op til de berørte virksomheder og myndigheder at beskytte menneskerettighederne – frem for selv at fastsætte detaljerede regler – og har dermed uddelegeret ansvaret for menneskerettighederne til de berørte aktører. Det giver fleksibilitet, men medfører også en vis deregulering og derfor mindre direkte demokratisk kontrol. Kritikken har da også været, særligt i relation til GDPR, at modellen bevæger sig væk fra den rettighedsbaserede tilgang, der i øvrigt kendetegner menneskeretten og databeskyttelsesretten, mod en risikobaseret regulering, hvor der hersker tvivl om, hvornår noget er en "risiko", og hvordan man skal forholde sig til den (Gellert, 2016, 2020; Malgieri & Santos, 2025).

Hertil kommer, at den fulde realisering af menneskerettighederne afhænger af, at den borger, der bliver berørt af et AI-system, bruger sine rettigheder efter AI-forordningen til forklaring og til at klage. Da det primære ansvar for menneskerettighederne nu ligger hos de berørte aktører, er det her afgørende, at de relevante myndigheder fører et effektivt tilsyn med de berørte virksomheder og myndigheder. EU-lovgiver kan med andre ord godt uddelegere det primære ansvar for menneskerettigheder, men EU og medlemsstaterne skal i sidste ende selv stå på mål for deres forpligtelser efter EU-chartret og EMRK, dvs. sikre at borgeres rettigheder er beskyttet.

Den risikobaserede tilgang kan ses som et forsøg på at sikre en beskyttelse af menneskerettighederne og samtidig fremme en fleksibel udbredelse af AI, idet det primære ansvar placeres hos dem, der anvender AI-systemerne. Spørgsmålet er, om vi derved sikrer en tilstrækkelig beskyttelse af borgerens rettigheder?

5. Den risikobaserede tilgang og demokrati

Fra et menneskeretligt perspektiv er den risikobaserede tilgang interessant, fordi den reelt operationaliserer den (soft law) "respekt" for grundlæggende rettigheder, der forventes af virksomhederne efter UNGP til en (hard law) juridisk forpligtelse til at foretage menneskeretlige konsekvensanalyser (Jørgensen et al., 2024). Idet AI-forordningen eksplicit inddrager menneskerettighederne i deres helhed, kan reguleringen i endnu højere grad, end det er tilfældet for GDPR (Oostveen & Irion, 2017), ses som andet og mere end EU-lovgivers håndtering af positive forpligtelser for de enkelte rettigheder.

Dette er i sig selv interessant, da menneskerettighederne som fastsat i forfatninger og i internationale og regionale konventioner traditionelt set er et anliggende for stater, ikke virksomheder. Det taler dog fint ind i EU-rettens traditionelle regulering af virksomheder, herunder krav om at de skal respektere grundrettigheder, og EU-lovgivers mission om at bringe særligt techgiganterne under demokratisk kontrol (Jørgensen et al., 2024). Forpligtelsen til at foretage konsekvensanalyser optræder således også i forordningen om Digital Service Act (Europa-Parlamentet og Rådet, 2022).

Selvom AI-forordningen ikke direkte pålægger udviklerne af AI-systemer (hvor de store tech-virksomheder typisk befinder sig) at lave en konsekvensanalyse, gælder kravet for alle dem, der anvender de omfattede højrisiko-AI-systemer. Reglerne skaber derfor et stærkt incitament for både dem, der anvender og udvikler AI-systemer, herunder techgiganterne, til at respektere borgerens grundlæggende rettigheder.

Fra et menneskeretligt perspektiv er det særdeles positivt, at både offentlige og private aktører forpligtes til at forholde sig til og håndtere de menneskeretlige konsekvenser af AI-systemer. Da virksomheder ikke i forvejen er direkte bundet af menneskerettighederne, må det antages at fungere som værn mod

virksomhedernes magt og bidrage til at sikre et værn om rettigheder og demokrati.

Den risikobaserede regulering flytter dog samtidig ansvaret for den menneskeretlige afvejning af, om AI-systemet konkret sikrer en rimelig balance mellem rettigheder og risici, fra lovgiver til dem, som anvender AI-systemet. Selv hvis man antager, at de berørte virksomheder er lige så kompetente til at foretage denne afvejning som lovgiver, så mindskes den menneskeretlige afvejnings demokratiske legitimitet.

For at sikre respekten for de grundlæggende rettigheder og demokratiet i en digital virkelighed, hvor AI spiller en stadig større rolle, flytter vi paradoksalt nok den menneskeretlige afvejning fra de demokratiske institutioner til dem, der anvender teknologien. Dette understreger vigtigheden af, at borgerne i kraft af de klagemekanismer, der findes i AI-forordningen (og GDPR), selv gør deres rettigheder gældende i forhold til beslutninger truffet med input fra AI-systemer.

6. Konklusion

Den stigende anvendelse af AI i både offentlige og private beslutningsprocesser udfordrer fundamentale menneskerettigheder og demokratisk legitimitet. EU's regulering – særligt GDPR og AI-forordningen – repræsenterer et ambitiøst forsøg på at operationalisere rettighedsbeskyttelse gennem en risikobaseret tilgang, der omfatter både myndigheder og virksomheder. Kravet om konsekvensanalyser udvider den menneskeretlige beskyttelse og styrker dermed borgerens position, men flytter samtidig ansvaret for den menneskeretlige afvejning fra lovgiver til de aktører, der anvender teknologien. Dette skaber et paradoks: Mens reguleringen sigter mod at fremme fleksibilitet og innovation, mindskes den demokratiske kontrol med, hvordan grundlæggende rettigheder beskyttes.

Spørgsmålet er, om de myndigheder og virksomheder, der anvender AI-systemer er i stand til at vurdere og håndtere den konkrete risiko for borgerens rettigheder, og om tilsynsmyndigheder og de berørte borgere er i stand til at reagere, hvis det ikke er tilfældet. Eller med andre ord, om EU's risikobaserede regulering af AI vitterligt formår at fastholde borgerens grundlæggende rettigheder som centrum i vores digitale samfund og demokrati. Tiden vil vise, om prisen for teknologisk fleksibilitet er for høj og reelt sker på bekostning af borgerens grundlæggende rettigheder.

Referencer

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press.

Den Europæiske Menneskerettighesdomstol (2008, 17. juli). I mod Finland, App. No. 20511/03 (2008), pr. 37 ff.

Den Europæiske Union (2016): Den Europæiske Unions Charter om Grundlæggende Rettigheder (C 202/02) konsolideret udgave. https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:12016P/TXT

De Gregorio, G. & Dunn P. (2022). The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age. *Common Market Law Review*, 59(2), 473-500. http://dx.doi.org/10.2139/ssrn.4071437

EU-Domstolen (2018, 6. november). Forenede sager C-569/16 og C-570/16 Bauer. EU:C:2018:871.

EU-Domstolen (2024a, 10. september). *Apple Sales International og Apple Operations Europe mod Europa-Kommissionen* (C465/20 P) EU:C:2024:724.

EU-Domstolen (2024b, 11. september). *Google og Alphabet mod Europa-Kommissionen* (C48/22 P) EU:C:2024:726.

Europa-Parlamentet og Rådet (2016). Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse). L 119/1. https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679

Europa-Parlamentet og Rådet (2022). Europa-Parlamentets og Rådets forordning (EU) 2022/2065 af 19. oktober 2022 om et indre marked for digitale tjenester og om ændring af direktiv 2000/31/EF (forordning om digitale tjenester). L 277/1. https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32022R2065

Europa-Parlamentet og Rådet (2024a). Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens og om ændring af forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 samt direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (forordningen om kunstig intelligens) (AI-forordningen) (2024) L 1/144. https://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX:32024R1689

Europa-Parlamentet og Rådet (2024b) Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed). L 1/81.

Europarådet (1950). *Den Europæiske Menneskerettighedskonvention*. https://www.echr.coe.int/documents/d/echr/convention_dan

Frantziou, E. (2019). (Most of) the Charter of Fundamental Rights is Horizontally Applicable. *European Constitutional Law Review*, 15(2), 306-323. https://doi.org/10.1017/S1574019619000166

Gellert, R. (2016). We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection. *European Data Protection Law Review*, 2(4), 481-492.

Gellert, R. (2020). *The Risk-Based Approach to Data Protection*. Oxford: Oxford University Press.

Jørgensen, R.F., Akhtar, M. & Koch, P.B. (2024). 'Business and Human Rights: Minimizing Risks or Maximizing Rights?' i G. De Gregorio, O. Pollicino & P. Valcke (red.) *The Oxford Handbook of Digital Constitutionalism*. Oxford: Oxford University Press.

Koch, I.E. (2005): Dichotomies, Trichotomies or Waves of Duties? *Human Rights Law Review*, 5(1), 81-103. https://doi.org/10.1093/hrlrev/ngi004

Malgieri, G. & Santos, C. (2025). Assessing the (severity of) impacts on fundamental rights. *Computer Law and Security Review*, 56(4). http://dx.doi.org/10.2139/ssrn.4875937

Oostveen, M. & Irion, K. (2017). 'The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Rights?' I Bakhoum, M. m.fl. (red.), *Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* Berlin: Springer.

Solove, D.J. (2025). *On Privacy and Technology*. Oxford: Oxford University Press 2025.

United Nations Human Rights Council (2011). United Nations Guiding Principles on Business and Human Rights (A/HRC/17/31).https://files.acquia.undp.org/public/migration/bizhumanrights/GuidingPrinciples-BusinessHR_EN.pdf

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.