

BELEIDSRAPPORT ‘DIGITAAL RACISME IN 2026’

Aanbevelingen voor de federale overheid

kif kif

Beleidsrapport 'Digitaal racisme in 2026'
Antwerpen, november 2026

Auteur
Igor Živković

Co-auteur
Anthony Mariën

Redactie en opmaak
Stef Arends
Nina Henkens

Coverfoto
Gijs de Boer

Uitgever
Kif Kif vzw
Statiestraat 139
2600 Berchem
Tel. 0456 87 33 21
info@kifkif.be
www.kifkif.be

Met dank aan Paola Verhaert en Oyidiya Oji voor inhoudelijke feedback op het rapport.

Creative Commons
Kif Kif juicht de verspreiding van kennis uit dit rapport toe, maar dringt aan op respect voor de auteur van de publicatie. We verzoeken iedereen die elementen uit het rapport wil overnemen dan ook om Kif Kif als bron te vermelden. Gebruik van dit rapport voor commerciële doeleinden mag alleen met toestemming van Kif Kif. Deze voorwaarden komen overeen met Creative Commons-licentie CC BY-NC-SA 4.0.

Dit rapport werd gemaakt met steun van de Cel Gelijke Kansen van de federale overheid.

_Equal.be

Inhoud

Samenvatting 3
Introductie 6
1. AI Act en de ‘Digital Omnibus’ 7
2. Online haat en anonimiteit 12
3. Online censuur van dissidente stemmen 19
4. Militarisering van artificiële intelligentie 22
5. Big Tech en een rechtvaardige digitale wereld 30
Conclusie 33

Samenvatting

Dit beleidsrapport analyseert vijf thema's inzake digitaal racisme, en formuleert in de eerste plaats beleidsaanbevelingen aan de federale overheid. Het rapport kan verder ook van belang zijn voor middenveldorganisaties, onderzoeksinstellingen en lokale overheden die meer willen weten over digitaal racisme en mogelijke beleidsmaatregelen.

AI Act en de 'Digital Omnibus'

Op Europees niveau domineert administratieve vereenvoudiging de beleidsagenda, ook op vlak van wetgeving inzake de digitale ruimte. In de praktijk is deze beleidsprioriteit vaak een vorm van deregulering, waarbij grote (technologie)bedrijven lobbyen om regelgeving af te zwakken. Zo is de AI Act, nog voor deze volledig van kracht is geworden, afgezwakt en aangepast met de AI Omnibus wetgeving. Verzwakte regelgeving kan de bescherming tegen racisme, discriminatie en mensenrechtenschendingen aantasten.

België heeft de verantwoordelijkheid om, ook binnen een veranderende Europese politieke context, vast te houden aan een wetgevend kader inzake AI dat de mensenrechten voorop stelt. Kif Kif vraagt onder andere om zo snel mogelijk officieel een AI-toezichthouder aan te stellen, om te investeren in de capaciteiten en samenwerkingsverbanden van de toezichthoudende instellingen, en een AI-register in te voeren voor overheden.

Online haat en anonimiteit

Online haat is een ernstig probleem voor gemarginaliseerde groepen. In de huidige beleidsvisie en wetsvoorstellen wordt de online anonimiteit van belagers aangeduid als een oorzaak, waardoor anonimiteit opgeheven moet worden. Maar anonimiteit is een fundamenteel onderdeel van het recht op vrije meningsuiting, dat belangrijke bescherming biedt aan burgers, inclusief aan gemarginaliseerde groepen. Tegelijkertijd is online haat een complex fenomeen dat ook van andere factoren afhankelijk is, zoals de politieke context, de algoritmes van sociale media en moderatiekeuzes.

Kif Kif beveelt aan om anonimiteit te waarborgen als democratisch grondrecht. Ook bevelen we aan om gerechtelijke ondersteuning van slachtoffers toegankelijker te maken, de huidige wetgeving, met name de Digital Services Act, strikter te handhaven, artikel 150 van de grondwet aan te passen, haatzaaiende politici verantwoordelijk te houden voor de gevolgen van hun haatcampagnes, en in te zetten op preventie.

Online censuur van dissidente stemmen

Een aanzienlijk deel van het publieke debat verloopt via sociale media. De algoritmes van sociale media en contentmoderatie op die platformen bepalen de manier waarop stemmen binnen dit debat aan bod komen. Vooral progressieve dissidente stemmen worden regelmatig gecensureerd op sociale media: hun content wordt zonder goede reden onzichtbaar gemaakt, of hun accounts worden geblokkeerd.

Kif Kif beveelt aan om via de Digital Services Act te blijven inzetten op verhoogde transparantie inzake de algoritmische aanbevelingssystemen en de rechten van gebruikers af te dwingen.

Militarisering van artificiële intelligentie

In een context van toenemende geopolitieke spanningen worden artificiële intelligentie en andere datagedreven technologieën zeer invloedrijk inzake nationale veiligheid en bij internationale conflicten. Er is een dubbele dynamiek ontstaan, waarbij civiele technologie wordt toegepast in militaire ruimtes, en militaire technologie in civiele ruimtes. Deze dynamiek vormt een gevaar voor de mensenrechten en de principes van antiracisme en non-discriminatie.

Kif Kif beveelt aan om bedrijven en technologieën die incompatibel zijn met mensenrechten te weren uit overheidsopdrachten en het gebruik ervan te verbieden. Ook bevelen we aan om een duidelijk juridisch kader te ontwikkelen dat de ontwikkeling en inzet van artificiële intelligentie en andere datagedreven technologieën binnen militaire toepassingen en het domein van nationale veiligheid reguleert, met aandacht voor de overgang van de civiele naar de militaire ruimte. De mensenrechten moeten daarbij vooropgesteld worden.

Big Tech en een rechtvaardige digitale wereld

Vandaag de dag is de digitale wereld grotendeels in handen van enkele grote, voornamelijk Amerikaanse, technologiebedrijven, ook wel bekend als Big Tech. De enorme concentratie van macht en rijkdom in dit kleine aantal bedrijven is een bedreiging voor de democratie en mensenrechten. Beleid moet zich richten op zowel het aanpakken van de marktmacht van Big Tech, als op het ondersteunen van alternatieven die het algemeen belang vooropstellen.

Kif Kif beveelt aan om op zowel Belgisch als Europees niveau bestaande beleidskaders inzake antimonopoliewetgeving strikt te handhaven, om op Europees niveau aanpassingen te vragen aan de Cloud and AI Development Act, om Big Tech te belasten op basis van digitale activiteit in

België, om een proces te starten om af te stappen van diensten van Big Tech binnen overheidsdiensten, en om alternatieve digitale technologieën te ondersteunen.

Om digitaal racisme tegen te gaan is een sterk en ambitieus beleid nodig: Europees moeten de DSA en DMA strikt worden gehandhaafd en mensenrechten vooropgesteld worden, terwijl België zelf lacunes kan opvullen met verschillende maatregelen, zoals een transparantieregister voor AI gebruikt door overheden, een verbod op biometrische massasurveillance en een wetgevend kader voor civiele AI in militaire contexten. Op termijn moeten structurele maatregelen de macht van Big Tech inperken, om zo een democratische en inclusieve digitale ruimte mogelijk te maken.

Introductie

Onze samenleving bevindt zich in een periode van versnelde technologische transformatie, waarbij artificiële intelligentie (AI) en datagedreven systemen steeds dieper geworteld raken in het dagelijkse leven van burgers. Tegelijkertijd groeit het kritisch besef dat digitale technologieën geen neutrale middelen zijn. Ze worden hoofdzakelijk vormgegeven door een kleine groep Amerikaanse technologiebedrijven, die zich steeds meer aansluiten bij extreemrechtse politieke visies. Daarbij zijn de winstmodellen van deze bedrijven al sinds het begin gebaseerd op manipulatieve algoritmes, uitbuiting en agressieve monopolievorming.

Racisme en discriminatie worden door deze technologieën dan ook regelmatig versterkt. Als antiracistische middenveldorganisatie met expertise in de digitale ruimte Kif Kif kreeg in 2024 en vervolgens in 2026 een subsidie van de dienst Gelijke Kansen van de federale overheid om de impact van dergelijke technologieën op racisme en discriminatie te onderzoeken en beleidsaanbevelingen te formuleren[1]. Reeds in 2024 verscheen de eerste beleidsbrief[2] waarin aanbevelingen werden geformuleerd om online haatspraak tegen te gaan en de AI Act correct te implementeren.

Dit beleidsrapport vormt een verdieping en verbreding van de eerste beleidsbrief. Vijf thema's inzake digitaal racisme worden in dit rapport uitgelicht:

1. AI Act en de 'Digital Omnibus'
2. Online haat en anonimiteit
3. Online censuur van dissidente stemmen
4. Militarisering van artificiële intelligentie
5. Big Tech en een rechtvaardige digitale wereld.

De beleidscontext om digitaal racisme het hoofd te bieden is uitdagend, gezien de complexiteit van deze dossiers en de macht van grote technologiebedrijven. Er is enerzijds nood aan zowel het onmiddellijk inperken van de negatieve invloed van AI en datagedreven systemen op discriminatie en racisme. Anderzijds is er ook nood aan structurele maatregelen die de digitale wereld herstructureren om compatibel te zijn met mensenrechten, non-discriminatie en de

[1] KB van 2 oktober 2023 betreffende de modaliteiten voor de toekenning van jaarlijkse subsidies aan verenigingen die strijden tegen racisme voor wat betreft de materies die behoren tot de bevoegdheid van de federale overheid.

[2] *Beleidsbrief Kif Kif 2.0 - Tegengaan van racisme in tijden van versnelde digitalisering en artificiële intelligentie*. (2024). https://drive.google.com/file/d/1pSk4tdPuM19d6biWl4RD1RCwy_R9WNYC/view?usp=sharing

democratie. Dit beleidsrapport is opgesteld in functie van beide doelstellingen. Wij hopen zo bij te dragen aan ambitieuze maar noodzakelijke beleidsmaatregelen om een rechtvaardige digitale wereld op te bouwen.

1. AI Act en de ‘Digital Omnibus’

Sinds de inwerkingtreding van de Europese AI Act in 2024 beschikt de Europese Unie voor het eerst over een horizontaal regelgevend kader voor artificiële intelligentie. De AI Act biedt belangrijke beschermingen aan Europese burgers, maar schiet desondanks ernstig tekort in het beschermen van mensenrechten[3]. Met name op vlak van het gebruik van AI door veiligheidsdiensten en overheidsdiensten in domeinen zoals de openbare veiligheid, de nationale veiligheid, asiel en migratie zijn er gebreken. Veel van de beschermings- en transparantievereisten voorzien in de AI Act zijn in deze domeinen niet van toepassing. Daarom is vooral voor gemarginaliseerde groepen zoals mensen met een migratieachtergrond, mensen van kleur en mensen op de vlucht er een zeer groot risico op mensenrechtenschendingen. Aanpassingen aan deze verordening zouden deze tekortkomingen moeten aanpakken..

Het is net daarom zorgwekkend dat recente politieke beslissingen mensenrechten nog lager plaatsen op de prioriteitenlijst. Nog voor de AI Act volledig van kracht werd, stelde de Europese Commissie een **Digital AI Omnibus** voor, die op 27 juli 2026 definitief van kracht ging. Dit pakket aan wetsvoorstellen wordt gepresenteerd als een manier om administratieve lasten voor bedrijven te verminderen en het Europese concurrentievermogen te versterken. De voorgestelde wijzigingen omvatten onder meer het uitstellen van bepaalde verplichtingen, het vereenvoudigen van conformiteitsprocedures en het aanpassen van verschillende verplichtingen voor ontwikkelaars en gebruikers van AI-systemen.

Volgens de Europese organisatie voor digitale rechten **EDRi** gaat deze vereenvoudiging echter veel verder dan administratieve efficiëntie. De organisatie waarschuwt dat de Omnibus een fundamentele verschuiving betekent van een op rechten gebaseerde benadering naar een concurrentiegerichte benadering, waarbij essentiële waarborgen rond transparantie, risicobeheer en publieke verantwoording worden afgezwakt. EDRi stelt dat de Europese Unie hiermee haar eigen digitalerechtenkader ondermijnt op een moment waarop AI een steeds grotere rol speelt in het dagelijkse leven.[4][5]

Ook **Corporate Europe Observatory** wijst erop dat de voorstellen tot stand kwamen onder sterke druk van grote technologiebedrijven, die al langer pleiten voor minder regelgeving en

---

[3] *EU’s AI Act fails to set gold standard for human rights*. (2024, April 4). European Digital Rights (EDRi). https://edri.org/our-work/eu-ai-act-fails-to-set-gold-standard-for-human-rights/

[4] *AI Omnibus deal: EU lawmakers should reject a rollback of AI safeguards*. (2026, Juni 11). European Digital Rights (EDRi). https://edri.org/our-work/ai-omnibus-deal-eu-lawmakers-should-reject-a-rollback-of-ai-safeguards/

[5] *Europe is dismantling its digital rights from within*. (2025, November 27). European Digital Rights (EDRi). https://edri.org/our-work/europe-is-dismantling-its-digital-rights-from-within/

meer flexibiliteit. Volgens hun onderzoek heeft de lobby van Big Tech een belangrijke invloed gehad op de richting van de hervormingen.[6]

De Belgische minister van Digitalisering **Vanessa Matz** schaarde zich achter het Omnibus-voorstel, onder een duidelijke voorwaarde: *"Ik sta volledig achter de vereenvoudiging van de lasten voor onze bedrijven, maar niet ten koste van de bescherming van persoonsgegevens. Vereenvoudiging mag niet leiden tot deregulering",*[7]

Kif Kif volgt echter EDRi en Corporate Europe Observatory in haar standpunt dat de Digital Omnibus wel degelijk een vorm van deregulering is die een zorgwekkend effect heeft op de strijd tegen racisme en discriminatie. Tal van onderzoeken[8] tonen namelijk aan dat AI-systemen bestaande maatschappelijke ongelijkheden kunnen reproduceren of versterken wanneer zij worden getraind op historisch bevooroordeelde datasets of wanneer zij onvoldoende worden getest op discriminerende effecten. Dat geldt onder meer voor toepassingen in:

- rekrutering;
- onderwijs;
- kredietverlening;
- sociale zekerheid;
- voorspellend politiewerk;
- grenscontrole;
- fraudedetectie;

Gemarginaliseerde groepen lopen daardoor een verhoogd risico op discriminatie en ongelijke behandeling. Juist daarom bevat de AI Act verschillende verplichtingen rond risicobeheer, documentatie, menselijke controle en de beoordeling van de impact op fundamentele rechten. Wanneer deze waarborgen worden uitgesteld of afgezwakt, neemt ook het risico toe dat discriminerende AI-systemen langer operationeel blijven zonder effectieve controle.

Voor België is dit bijzonder relevant. Overheden, publieke instellingen en bedrijven gebruiken steeds vaker AI-toepassingen. Een sterke implementatie van de AI Act kan bijdragen aan de bestrijding van structurele discriminatie; een afzwakking ervan dreigt bestaande ongelijkheden

---

[6] *Article by article, how Big Tech shaped the EU's roll-back of digital rights*. (2026, Januari 14). https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights

[7] *Omnibusverordening rond artificiële intelligentie: België steunt het voorstel van de Europese Commissie*. (2026, Maart 12). https://matz.belgium.be/nl/nieuws/omnibusverordening-rond-artificiele-intelligentie-belgie-steunt-het-voorstel-van-de-europese

[8] Zie bijvoorbeeld: European Union Agency for Fundamental Rights. (2022). *Bias in algorithms: Artificial intelligence and discrimination*. Publications Office of the European Union.

verder te institutionaliseren. De AI Omnibus bevat met andere woorden een aantal duidelijke risico's en negatieve gevolgen:

1. Minder bescherming tegen algoritmische discriminatie

Een versoepeling van de verplichtingen voor aanbieders van AI systemen met een hoog risico vermindert de mogelijkheden om discriminerende systemen tijdig op te sporen en te corrigeren. Wanneer verplichtingen rond documentatie, audits en transparantie worden afgezwakt, wordt het voor toezichthouders, onderzoekers, journalisten en middenveldorganisaties namelijk moeilijker om AI-systemen kritisch te evalueren of discriminerende praktijken aan het licht te brengen.

Vooral groepen die vandaag reeds disproportioneel worden getroffen door discriminatie lopen hierdoor extra risico. De Omnibus stelt bovendien de verplichting van essentiële waarborgen voor hoogrisico-AI-systemen uit naar een latere datum. Hierdoor dreigen discriminerende AI-toepassingen langer ingezet te worden zonder de noodzakelijke transparantie, menselijke controle en bescherming van fundamentele rechten.[9]

2. Uitholling van het Europese mensenrechtenmodel

De Europese Unie profileerde zich internationaal als voortrekker van een mensgerichte AI-regulering. Een snelle deregulering nog vóór de AI Act volledig is geïmplementeerd ondermijnt de geloofwaardigheid van dat model en creëert rechtsonzekerheid voor overheden, bedrijven en burgers. Het schept bovendien een precedent: wanneer recent aangenomen wetgeving inzake digitale rechten (en andere wetgeving) opnieuw kan worden herzien nog vóór zij in werking treedt, ontstaat het risico dat actoren de implementatiefase aangrijpen als een tweede gelegenheid om ongewenste regelgeving af te zwakken.

3. Uitholling van de bescherming van gevoelige persoonsgegevens

De AI Omnibus verruimt de mogelijkheden om bijzondere categorieën van persoonsgegevens – zoals gegevens over etnische afkomst, gezondheid, politieke overtuiging of seksuele oriëntatie – te verwerken voor biasdetectie en -correctie. Hoewel

[9] *AI Omnibus deal: EU lawmakers should reject a rollback of AI safeguards*. (2026, Juni 11). European Digital Rights (EDRi).
https://edri.org/our-work/ai-omnibus-deal-eu-lawmakers-should-reject-a-rollback-of-ai-safeguards/

het bestrijden van algoritmische bias belangrijk is, dreigt deze uitzondering de strikte bescherming van gevoelige persoonsgegevens onder de GDPR uit te hollen en het gebruik van dergelijke gegevens in AI-systemen te normaliseren.

Daarom formuleert Kif Kif de volgende aanbevelingen:

1. Verdedig op rechten gebaseerde wetgeving inzake digitale activiteiten

Administratieve vereenvoudiging mag nooit leiden tot een verminderde rechtsbescherming. We stellen vast dat dit in de praktijk echter wel het geval is, zoals hierboven beschreven. België moet zich in de toekomst tijdens Europese onderhandelingen blijven verzetten tegen elke aanpassing van wetgeving die fundamentele rechten, non-discriminatie of transparantie afzwakt, inclusief inzake de toekomstige Data Omnibus[10]. Ook moet België blijven aandringen op sterke mensenrechtenwaarborgen bij het ontwerp van toekomstige wetgeving, ook voor veiligheids -en overheidsdiensten in domeinen inzake openbare veiligheid, nationale veiligheid, asiel en migratie.

2. Versterk het toezicht op algoritmische discriminatie

Door vertraging in de aanstelling van de AI-toezichthouder is er momenteel een juridisch vacuüm. Dit leidt tot een gebrek aan bescherming voor burgers en gebrek aan een effectief klachtenmechanisme, wat ernstige gevolgen kan hebben voor de fundamentele mensenrechten. Zorg dat het Belgisch Instituut voor Post en Telecommunicatie Diensten (BIPT) zo snel mogelijk officieel wordt aangesteld als AI toezichthouder en garandeer voldoende middelen en mensenrechtenexpertise binnen deze dienst. Zorg ook voor een duidelijke verdeling van regionale en federale bevoegdheden die de bescherming van mensenrechten prioriteert, met vaste samenwerkingsprotocollen tussen de diensten op verschillende beleidsniveaus.

België telt 27 autoriteiten belast met de bescherming van de grondrechten krachtens artikel 77 van AI Act, verdeeld onder verschillende domeinen en beleidsniveaus. Deze versnippering riskeert onduidelijkheid en ontoegankelijkheid voor de burger, en gebrekkig toezicht op algoritmische discriminatie. Zorg voor één duidelijk aanspreekpunt voor de burger inzake mensenrechtenschendingen door AI, dat de burger ondersteunt en begeleidt. Versterk ook de samenwerking tussen het BIPT, autoriteiten belast met de bescherming van grondrechten en de Gegevensbeschermingsautoriteit om een vlotte uitwisseling van informatie en dienstverlening naar de burger toe te garanderen. Daarbij

[10] *Why the Digital Omnibus puts GDPR and ePrivacy at risk*. (2025, November 19). European Digital Rights (EDRi). https://edri.org/our-work/why-the-digital-omnibus-puts-gdpr-and-eprivacy-at-risk/

moeten deze instanties beschikken over voldoende middelen, gedeelde expertise en duidelijke samenwerkingsprotocollen om algoritmische discriminatie effectief op te sporen en aan te pakken.

3. Voer een verplicht publiek AI-register in voor alle overheidsdiensten

Zorg, naar Nederlands voorbeeld[11] dat alle overheden, inclusief veiligheidsdiensten, verplicht hun AI systemen moeten registreren in een centraal register. Maak dit register toegankelijk en gebruiksvriendelijk, om zo maximale transparantie voor de burger te waarborgen en discriminatie door AI-systemen sneller op te sporen. Daarbij moeten alle fasen van het softwareontwerp traceerbaar zijn, van gegevensverzameling tot productie. Door zo niet alleen aan te sluiten bij de vereisten van de AI-Act inzake hoogrisico-AI systemen maar ook laagrisico-AI systemen en AI systemen in gebruik bij veiligheidsdiensten te rapporteren, geeft de overheid het goede voorbeeld en een sterk signaal naar de burgers over verantwoord en transparant gebruik van AI.

4. Investeer in onafhankelijke expertise en onderzoek

België moet structureel investeren in interdisciplinair wetenschappelijk onderzoek naar algoritmische discriminatie, AI-governance en digitale rechten, zodat beleidsmakers hun beslissingen kunnen baseren op onafhankelijke wetenschappelijke expertise. Het middenveld moet daarin erkend worden als volwaardige speler en partner met waardevolle expertise, ervaring en onderzoeksvaardigheden. Investeer in capaciteitsopbouw van maatschappelijke actoren om AI systemen door te lichten en zo opsporing van discriminatie te faciliteren.

5. Betrek het middenveld structureel bij AI-beleid

Antiracistische organisaties, mensenrechtenorganisaties, consumentenverenigingen en andere maatschappelijke actoren moeten systematisch betrokken worden bij de ontwikkeling, evaluatie en implementatie van AI-beleid. Hun expertise is essentieel om de maatschappelijke impact van AI correct in te schatten.

[11] *Het algoritmeregister van de Nederlandse overheid*. (n.d.). https://algoritmes.overheid.nl/nl

2. Online haat en anonimiteit

Online haat vormt een groeiende bedreiging voor de democratische rechtsstaat, de vrijheid van meningsuiting en de veiligheid van burgers.

Onderzoek van Kif Kif[12] toont aan dat personen met een migratieachtergrond en andere gemarginaliseerde groepen in België disproportioneel doelwit zijn van online haatcampagnes. Online haatspraak gebeurt soms spontaan door individuen, maar komt ook vaak voort uit systematische haatcampagnes. Dergelijke online haatcampagnes, die inspelen op racistische en seksistische stereotypen en vooroordelen, worden niet zelden georchestreerd uit politieke hoek om electorale redenen, en wakkeren online haat verder aan.

Een cruciale versterkende factor zijn de algoritmes van sociale mediaplatformen, die ontworpen zijn om aandacht en engagement te maximaliseren. Emotionele, haatdragende en schokkende berichten krijgen daardoor vaak algoritmische voorrang op genuanceerde inhoud. Daarnaast spelen gebrekkige moderatie van sociale media en beperkte handhaving van bestaande wetgeving een belangrijke rol.

Online haat draagt uiteindelijk bij aan bredere processen van ontmenselijking, normalisering van discriminatie en maatschappelijke polarisatie. Recent onderzoek van **ECRI (Europese Commissie tegen Racisme en Intolerantie)** toont aan dat online haat toeneemt en steeds vaker gedoogd wordt[13]. Om veilige online ruimtes voor iedereen te waarborgen is het essentieel dat beleid zich niet uitsluitend richt op individuele gebruikers, maar ook op de systemen die haat versterken en economisch rendabel maken.

Anonimiteit wordt vaak aangehaald als het grootste probleem in de strijd tegen online haat. Maar anonimiteit is niet enkel een zeer beperkte oorzaak van online haat, het is voor veel mensen net een noodzakelijke voorwaarde om zich uit te spreken over racisme en discriminatie. Activisten, slachtoffers van racisme, klokkenluiders, journalisten en mensen die vrezen voor represailles kunnen vaak enkel veilig deelnemen aan het publieke debat wanneer zij hun identiteit niet onmiddellijk hoeven prijs te geven. Zoals **Bits of Freedom** benadrukt[14], is anonimiteit geen afwijking van de democratie, maar juist een voorwaarde om vrij aan die democratie te kunnen deelnemen.

---

[12] *"Online haat is een winstmodel en een electoraal instrument."* (n.d.). Kif Kif. https://www.kifkif.be/bijdragen/online-haat-is-een-winstmodel-en-een-electoraal-instrument

[13] Council of Europe. (2026). *Annual report on ECRI's activities covering the period from 1 January to 31 December 2025*. rm.coe.int

[14] *Anonimiteit is onmisbaar* (2021, Maart 22). Bits of Freedom. https://www.bitsoffreedom.nl/2021/03/22/anonimiteit-is-onmisbaar/

Verschillende aangekondigde beleidsmaatregelen in België hebben voorgesteld om de online anonimiteit in te perken als antwoord op online haat. Ook wordt de opheffing van anonimiteit via verplichte digitale identificatie voorgesteld als maatregel om een leeftijdsgrens te kunnen handhaven voor toegang tot sociale media, om zo jongeren en kinderen te beschermen tegen de schadelijke effecten van sociale media.

Zo is er het voorstel van resolutie van 12 september 2025 “betreffende de opheffing van online anonimiteit en de instelling van een doeltreffende leeftijdscontrole voor toegang tot sociale media”. Dit voorstel had als als hoofddoelstelling een algemene opheffing van de anonimiteit op sociale media door middel van verplichte registratie vooraf, en leeftijdscontroles voor minderjarigen in te stellen om hen te beschermen tegen de schadelijke effecten van sociale media, inclusief online haat. Daarnaast bepleitte minister Matz recent ook de opheffing van ‘kwaadwillige anonimiteit’ en een invoering van een leeftijdsgrens voor sociale media, met controle door digitale identificatie-apps zoals ItsMe[15]. Tot slot werd recent een wetsvoorstel van minister Beenders en minister Matz om de anonimiteit van online gebruikers te beperken door slachtoffers van online haat toegang te geven tot de identiteit van anonieme accounts, goedgekeurd door de regering.

Het **Federaal Instituut voor de Rechten van de Mens (FIRM)** waarschuwt echter dat anonimiteit een fundamenteel onderdeel vormt van de vrijheid van meningsuiting en slechts in uitzonderlijke omstandigheden mag worden doorbroken. Volgens het FIRM moeten maatregelen tegen online haat steeds noodzakelijk, proportioneel en voorzien zijn in de wet. Het instituut benadrukt bovendien dat bestaande juridische instrumenten reeds mogelijkheden bieden om de identiteit van gebruikers op te vragen wanneer dit gerechtvaardigd is door een gerechtelijk onderzoek.[16]

Ook de **Ligue des Droits Humains** bekritiseert voorstellen die anonimiteit structureel willen terugdringen. Volgens de Ligue vertrekken dergelijke voorstellen van een verkeerde diagnose. Online haat wordt niet veroorzaakt door anonimiteit op zich, maar door een combinatie van het ontwerp van sociale mediaplatformen, maatschappelijke polarisatie, onvoldoende moderatie en politieke dynamieken. Het structureel afbouwen van anonimiteit dreigt vooral fundamentele

[15] Mayda, K. (2026, Juli 24). Minister Matz wil Frans voorbeeld volgen met socialemediaverbod tot 15 jaar, maar botst op N-VA. *De Standaard*. https://www.standaard.be/politiek/minister-matz-wil-frans-voorbeeld-volgen-met-socialemediaverbod-tot-15-jaar-maar-botst-op-n-va/159141083.html

[16] Federaal Instituut voor de bescherming en de bevordering van de Rechten van de Mens. (2026). *Advies over het voorstel van resolutie betreffende de opheffing van online anonimiteit en de instelling van een doeltreffende leeftijdscontrole voor toegang tot sociale media*. https://federaalinstituutmensenrechten.be/sites/default/files/2026-03/2026-FIRM-IFDH-Advies-anonimiteit-2-2026.pdf

rechten aan te tasten zonder de onderliggende oorzaken van online haat daadwerkelijk aan te pakken.[17]

Op vlak van reeds bestaande wetgeving ter bestrijding van online haat beschikt de Europese Unie sinds 2024 over een belangrijk regelgevend kader via de **Digital Services Act (DSA)**. De DSA verplicht zeer grote online platformen (platformen met meer dan 45 miljoen gebruikers in de EU) onder meer om systemische risico's – waaronder de verspreiding van illegale inhoud, haatspraak en maatschappelijke polarisatie – in kaart te brengen en te beperken. Daarnaast voorziet de DSA in transparantieverplichtingen, onafhankelijke audits, meldingsmechanismen en toegang voor onderzoekers tot platformgegevens.

De uitdaging voor België bestaat vandaag dan ook minder uit het creëren van nieuwe maatregelen die mensenrechten riskeren te beperken, zoals het inperken van de anonimiteit, dan uit een effectieve implementatie en handhaving van de bestaande Europese regelgeving.

De voorstellen die anonimiteit willen opheffen ter bestrijding van online haat en om leeftijdsgrenzen op te leggen voor sociale media, bevatten volgens Kif Kif dus verschillende risico's en problemen:

1. Verkeerde probleemdefinitie

Door anonimiteit als hoofdoorzaak van online haat te beschouwen, verschuift de verantwoordelijkheid weg van de online platformen die hun systemen bewust optimaliseren voor maximale aandacht en engagement, en van haat aangestuurd uit politieke hoek. Hierdoor blijven de fundamentele ontwerpkeuzes van sociale media en de verantwoordelijkheid van politici grotendeels buiten beeld.

2. Aantasting van fundamentele rechten

Huidige identificatiesystemen om de anonieme toegang tot digitale diensten te beperken, vormen zeer ingrijpende en vergaande inbreuken op de privacy en burgerrechten. Identificatiesystemen zoals ItsMe koppelen aan sociale media brengt aanzienlijke risico's met zich mee inzake gegevensbescherming, datalekken en *function creep*. Een algemene beperking van anonimiteit kan dan ook leiden tot een afschrikwekkend effect (ook wel 'chilling effect') op de vrijheid van meningsuiting. Vooral journalisten, mensenrechtenverdedigers, activisten en gemarginaliseerde groepen lopen het risico zich uit het publieke debat terug te trekken.

[17] Ligue des droits humains. (2026). *Anonymat en ligne ét vérification de l'âge*. https://www.archive.liguedh.be/wp-content/uploads/2026/03/Analyse-anonymat-2026-1.pdf

3. Beperkte effectiviteit

Er bestaat weinig empirisch bewijs dat het afschaffen van anonimiteit op zichzelf leidt tot een substantiële vermindering van online haat. Personen die doelbewust illegale haat verspreiden kunnen uitwijken naar andere platformen, gebruik maken van VPN-diensten of valse identiteiten aanmaken. De maatregelen dreigen daardoor vooral de privacy van gewone burgers te beperken zonder de meest problematische actoren effectief te treffen.

4. Onvoldoende benutting van bestaande regelgeving

Er bestaat reeds een belangrijke Europese verordening, de Digital Services Act, om online haat tegen te gaan. Daarnaast is er ook zijn er in België reeds de antiracismewet, de antidiscriminatiewet en de genderwet die haatspraak die aanzet tot geweld, vijandigheid of discriminatie strafbaar maakt. De prioriteit moet zijn om deze regelgeving optimaal te benutten en te handhaven.

5. Onvoldoende rechtswaarborgen en onduidelijke criteria bij het opheffen van anonimiteit

Kif Kif is van mening dat het recente wetsvoorstel betreffende het opheffen van de anonimiteit via de Ombudsdienst in huidige vorm onvoldoende rechtswaarborgen biedt. Hoewel anonimiteit van individuen in zeer concrete gevallen opgeheven kan worden, is dit een discretionaire bevoegdheid die een exclusieve verantwoordelijkheid van de politie of het gerecht zou moeten zijn. Daarbij zijn de criteria over welke uitingen gelden als kwaadwillige interpersoonlijke communicatie niet genoeg gepreciseerd, waardoor ook personen die legitieme uitingen stellen, riskeren hun anonimiteit te verliezen. Ook riskeert deze maatregel disproportionele verantwoordelijkheid te leggen bij de slachtoffers van online haat, in plaats van bij socialemediabedrijven (cfr. probleemdefinitie 1).

Daarom formuleert Kif Kif de volgende aanbevelingen:

1. Behoud anonimiteit als democratisch uitgangspunt

België moet het principe verdedigen dat anonimiteit online een essentieel onderdeel vormt van de vrijheid van meningsuiting. Bovendien beschikt Justitie vandaag al over instrumenten om, onder de bestaande wettelijke voorwaarden, identiteitsgegevens op te vragen.

2. Maak gerechtelijke procedures toegankelijker voor slachtoffers

Slachtoffers van online haat moeten sneller en eenvoudiger toegang krijgen tot rechtsmiddelen. Dit omvat onder meer:

- laagdrempelige procedures om illegale inhoud te laten verwijderen;
- procedures die de de anonimiteit en veiligheid van slachtoffers garanderen wanneer melding wordt gemaakt bij de politie van online haat;
- snellere procedures voor rectificaties en schadevergoedingen;
- spoedprocedures voor ernstige bedreigingen, oproepen tot geweld en andere manifest onwettige inhoud;
- gespecialiseerde ondersteuning voor slachtoffers van online haat.

3. Versterk de handhaving van de Digital Services Act

België moet maximaal inzetten op een robuuste uitvoering van de DSA door:

- Voldoende middelen toe te kennen aan het Belgisch Instituut voor Post en Telecommunicatie Diensten (BIPT);
- Nauwe samenwerking te organiseren tussen het Belgisch Instituut voor Post en Telecommunicatiediensten, de Gegevensbeschermingsautoriteit, Unia, het Vlaams Mensenrechteninstituut (VMRI), het Federaal Instituut voor de Rechten van de Mens (FIRM), Instituut voor Gelijkheid van Vrouwen en Mannen (IGVM), de regionale bevoegde autoriteiten (VRM (Vlaamse Regulator voor de Media); CSA (Conseil Supérieur de l'Audiovisuel) en Medienrat) en Justitie, alsook met gelijkaardige actoren uit andere Europese lidstaten;
- Systematisch gebruik te maken van de onderzoeks- en handhavingsmechanismen die de DSA reeds voorziet om zo een strikte toepassing van de verplichtingen over systemische risico's te handhaven;
- Op Europees niveau de Commissie aansporen om duidelijkere richtlijnen over de rapportagevereisten in te voeren, inclusief duidelijkere informatie over hoe de huidige aanbevelingsalgoritmes samenhangen met systemische risico's, en meer aandacht voor systemische risico's voor fundamentele rechten[18];
- Actief deel te nemen aan Europese onderzoeken naar systemische risico's op grote online platformen en moderatie van online haat, met ondersteuning van de capaciteiten van mensenrechten- en middenveldorganisaties om onafhankelijke audits uit te voeren. Publiceer toegankelijke analyses over de verspreiding van haatspraak op de verschillende socialemediaplatformen.

[18] *Five lessons from three years of risk assessments*. (2026, Maart 18). European Digital Rights (EDRi). https://edri.org/our-work/five-lessons-from-three-years-of-risk-assessments-under-the-digital-services-act/

Harmoniseer ook de verschillende nationale wetgevingen inzake haatspraak binnen de EU. Een harmonisering zorgt voor een consistente aanpak tegen haatspraak en versterkt de mogelijkheden om op te treden tegen online haat op sociale media.

Daarnaast kan ook de Digital Markets Act de strijd tegen online haat versterken door de interoperabiliteit die reeds verplicht is voor berichtendiensten, uit te breiden naar sociale media. Zo kunnen gebruikers van sociale media overstappen naar andere diensten zonder het verlies van sociale contacten wanneer een platform hen onvoldoende beschermt tegen online haat.

4. Investeer in maatschappelijke preventie

Online haat is niet uitsluitend een technologisch probleem. Er is nood om meer aandacht te besteden aan de structurele oorzaken van racisme, seksisme en andere vormen van haat en uitsluiting. Daarbij moet er aandacht zijn voor meervoudige discriminatie. Daarom moet de federale overheid investeren in bijkomende acties, zoals :

- Antiracistische educatie met intersectionele lens;
- Mediawijsheid en digitale geletterdheid, inclusief de verantwoordelijkheid van digitale platformen over hun ontwerpkeuzes, moderatiepraktijken, aanbevelingssystemen;
- Sensibiliseringscampagnes die haatspraak maatschappelijk onaanvaardbaar maken en de aandacht vestigen op structurele oorzaken van (online) haat.

5. Zorg ervoor dat aanzetten tot haat strafbaar blijft

Kif Kif wil het belang benadrukken van ‘aanzetten tot haat’ te behouden als misdrijf. Recent werd door enkele politici een betoog gehouden om ‘aanzetten tot haat’ uit de antiracismewet te halen[19]. Eerder werd het wetsvoorstel nr. 2606/001 ingediend om ‘aanzetten tot haat’ in te perken of zelfs uit het strafrecht te halen. Dit gaat in tegen Europese en internationale wetgeving en verdragen, onder andere het Europese Kaderbesluit 2008/913. Een dergelijke wet zou ook een aantasting zijn van de Belgische rechtsstaat, zoals beoordeeld in een rapport van de Orde van Vlaamse Balies. Bovendien vormt haatspraak een ernstige bedreiging voor zowel de mentale als de fysieke gezondheid van burgers. Kif Kif wil daarbij benadrukken dat online haat niet enkel een

[19]Schillewaert, N. (2026, Mei 28). Waarom het (geen) zin heeft om de Belgische wetgeving rond “aanzetten tot haat” te wijzigen. *VRT NWS*.
https://www.vrt.be/vrtnws/nl/2026/05/28/discussie-over-bepaling-aanzetten-tot-haat/

individueel probleem is. Online haat is namelijk ook een politiek wapen om mensen uit de gemarginaliseerde groepen de mond te snoeren en te weren uit het publieke debat. ‘Aanzetten tot haat’ uit het strafrecht halen zou dus zorgen voor een aantasting van de publieke ruimte en democratische meningsverschillen, en vormt een bedreiging voor burgers.

6. Herzie Artikel 150 van de Grondwet

Het antiracistische middenveld en Unia pleiten al jaren voor een herziening van Artikel 150 van de Grondwet. Dit artikel, dat de bedoeling heeft om de vrijheid van meningsuiting van álle burgers te vrijwaren, bepaalt dat ‘het uiten van strafbare meningen via de pers’ berecht moet worden door een Hof van Assisen, met een volksjury. Gezien deze processen veel middelen vereisen, worden veel gevallen van online haat nooit effectief bestraft. Bovendien wordt haatspraak in tekstvorm op sociale media anders berecht dan haatspraak in videoformaat, waardoor veel gevallen van haat in tekstvorm niet bestraft worden. Kif Kif beveelt dus met klem aan om Artikel 150 aan te passen zodat álle haatspraak onder bevoegdheid van de correctionele rechtbank valt, en dat daarbij dezelfde regels gelden voor tekst en video. Deze aanpassing is cruciaal om haatspraak effectief te bestrijden.

7. Politici en partijen die haat zaaien moeten verantwoordelijk worden gehouden

Politici hebben een grote invloed op de publieke opinie en het behoeden van de rechtsstaat en dienen geresponsabiliseerd te worden inzake het aanzetten tot haat. Onderzoek van Kif Kif heeft uitgewezen dat sommige partijen en politici met opzet haat zaaien omwille van politieke doeleinden. Kif Kif volgt de aanbeveling van de Europese Commissie tegen Racisme & Discriminatie om te zorgen voor een wettelijke verplichting om publieke financiering stop te zetten van organisaties en partijen die racisme promoten[20]. Daarnaast vraagt Kif Kif aan politici om politieke verantwoordelijkheid te nemen bij racistische uitlatingen, en politici te schorsen indien ze haatuitspraken doen.

[20] European Commission against Racism and Intolerance. (2016). *General policy recommendation No. 15 on combating hate speech.* Council of Europe. https://rm.coe.int/ecri-general-policy-recommendation-no-15-on-combating-hate-speech/16808b5b01

3. Online censuur van dissidente stemmen

Sociale media zijn uitgegroeid tot een belangrijke publieke ruimte voor maatschappelijk debat, politieke mobilisatie en activisme. De manier waarop platformen content aanbevelen, rangschikken en modereren bepaalt in grote mate welke stemmen zichtbaar worden en welke niet. Daarbij is contentmoderatie, zoals het verwijderen of beperken van illegale inhoud, een belangrijke verantwoordelijkheid van deze platformen. Die contentmoderatie werkt momenteel niet alleen onvoldoende, sterker nog, ze wordt ook ingezet om legitieme content of accounts zonder voldoende transparantie of rechtsbescherming te verwijderen of in hun bereik te beperken. Recent werden accounts uit de LGBTQ+-gemeenschap bijvoorbeeld geblokkeerd zonder reden[21]. In dat geval spreken we van **online censuur**: legitieme maatschappelijke of politieke meningsuiting die op een ondoorzichtige of disproportionele manier worden beperkt.

Een specifieke vorm hiervan is **shadowbanning**: het systematisch beperken van de zichtbaarheid van accounts of berichten zonder dat gebruikers hiervan op de hoogte worden gebracht. Shadowbanning verschilt van klassieke contentmoderatie doordat inhoud niet noodzakelijk wordt verwijderd, maar wel aanzienlijk minder wordt verspreid via aanbevelingsalgoritmes, zoekresultaten of hashtags.

Mensenrechtenorganisaties zoals **Human Rights Watch** en **7amleh** (The Arab Center for the Advancement of Social Media) documenteerden honderden gevallen waarbij vooral Palestijnse en antiracistische content en content rond mensenrechtenactivisme disproportioneel werd beperkt op Meta-platformen. Volgens Human Rights Watch ging het om een "systemische en wereldwijde censuur" van Palestijns-gerelateerde content, waarbij accounts werden beperkt zonder transparante motivering of effectieve beroepsmogelijkheden.[22]

Wanneer algoritmes systematisch bepaalde maatschappelijke thema's of gemeenschappen minder zichtbaar maken, ontstaat een risico op digitale uitsluiting. Met andere woorden, niet alleen individuele accounts worden geraakt, maar ook het maatschappelijke debat. Minder zichtbaarheid betekent minder bereik, minder politieke invloed en minder mogelijkheden om discriminatie, racisme en mensenrechtenschendingen publiek onder de aandacht te brengen.

De **Digital Services Act (DSA)** bevat belangrijke waarborgen tegen willekeurige contentmoderatie. De DSA verplicht platformen om gebruikers te informeren wanneer content wordt verwijderd of de zichtbaarheid ervan wordt beperkt. Gebruikers moeten bovendien

[21] *Brief aan Meta: stop met willekeurige accountblokkades*. (2026, Mei 20). Bits of Freedom. https://www.bitsoffreedom.nl/2026/05/20/brief-aan-meta-stop-met-willekeurige-accountblokkades/
[22] Human Rights Watch. (2023). *Meta's Broken Promises: Systemic censorship of Palestine content on Instagram and Facebook*. https://www.hrw.org/sites/default/files/media_2023/12/ip_meta1223%20web.pdf

toegang krijgen tot een interne klachtenprocedure en een onafhankelijke buitengerechtelijke geschillenregeling. Zeer grote online platformen moeten daarnaast de maatschappelijke risico's van hun aanbevelingssystemen beoordelen en maatregelen nemen om die risico's te beperken. De DSA verbiedt shadowbanning echter niet expliciet. De bescherming bestaat vooral uit transparantieverplichtingen, rechtsbescherming voor gebruikers en toezicht op aanbevelingsalgoritmen.

Tot slot zien we een bredere evolutie waarbij maatschappelijke organisaties steeds meer onder druk komen te staan om zich aan te passen aan de logica van sociale media. Om zichtbaar te blijven moet de communicatie afgestemd worden op commerciële algoritmen: persoonlijke storytelling, emotionele boodschappen, virale formats en algoritmevriendelijke content. Hierdoor verschuift maatschappelijke communicatie steeds meer van genuanceerde maatschappelijke analyse via inhoudelijke argumentatie naar content die is geoptimaliseerd voor de aandachtseconomie. Dit dreigt niet alleen de kwaliteit van het publieke debat, maar ook het collectieve karakter van sociale bewegingen te ondermijnen.

Daarom formuleert Kif Kif de volgende aanbevelingen:

1. Versterk de handhaving van de Digital Services Act

België moet de bestaande mogelijkheden van de DSA maximaal benutten door de capaciteit van het BIPT als Digital Services Coordinator verder uit te bouwen en nauw samen te werken met de Europese Commissie bij onderzoeken naar systemische moderatieproblemen op zeer grote online platformen.

2. Versterk de rechtsbescherming van gebruikers

België moet actief de gebruikersrechten waarborgen die reeds in de DSA zijn opgenomen. Gebruikers moeten eenvoudig bezwaar kunnen maken tegen accountbeperkingen, aanbevelingsbeperkingen of andere moderatiemaatregelen en toegang hebben tot snelle, onafhankelijke geschillenbeslechting.

3. Investeer in onafhankelijk onderzoek naar moderatie op socialemediaplatformen en algoritmische discriminatie

De federale overheid moet investeren in onafhankelijk onderzoek naar shadowbanning, algoritmische discriminatie en de maatschappelijke impact van aanbevelingssystemen. Daarbij moet bijzondere aandacht gaan naar de ervaringen van geracialiseerde gemeenschappen, mensenrechtenverdedigers en maatschappelijke organisaties.

4. Pleit op Europees niveau voor meer transparantie over aanbevelingsalgoritmen

België moet binnen de Europese Unie pleiten voor bijkomende transparantieverplichtingen rond aanbevelingssystemen, zodat gebruikers beter kunnen begrijpen waarom content minder zichtbaar wordt en onderzoekers gemakkelijker systematische patronen van shadowbanning kunnen detecteren.

5. Versterk de rol van maatschappelijke organisaties binnen het DSA-toezicht

België moet antiracistische organisaties, mensenrechtenorganisaties en onafhankelijke onderzoekers structureel ondersteunen om de maatschappelijke risico's van grote onlineplatformen te monitoren. Hun expertise is noodzakelijk om systematische vormen van digitale uitsluiting tijdig te detecteren.

6. Zorg dat gebruikers kunnen kiezen voor een aanbevelingssysteem dat niet gebaseerd is op profilering.

België moet de bepalingen van artikel 38 van de DSA strikt handhaven en er bij de Europese Commissie op aandringen dat die erop toeziet dat grote onlineplatformen de keuze voor een niet-geprofileerd aanbevelingssysteem eenvoudig toegankelijk en gebruiksvriendelijk maken. Zo worden burgers en maatschappelijke organisaties minder afhankelijk van commerciële aanbevelingsalgoritmen die emotionele, polariserende en virale content bevoordelen ten koste van genuanceerde maatschappelijke analyse.[23]

[23] *Rechter geeft Bits of Freedom opnieuw gelijk: blijvende keuzevrijheid voor gebruikers Instagram en Facebook* (2026, Maart 10). Bits of Freedom. https://www.bitsoffreedom.nl/pers/rechter-geeft-bits-of-freedom-opnieuw-gelijk-blijvende-keuzevrijheid-voor-gebruikers-instagram-en-facebook/

4. Militarisering van artificiële intelligentie

De wereld bevindt zich vandaag in een context van geopolitieke spanningen, militarisering en wapenwedloop. Enkele belangrijke conflicten zijn de oorlog en oorlogsmisdaden van Rusland tegen Oekraïne[24], de genocide die Israël pleegt in Gaza[25] en de oorlogsmisdaden van Israël in Libanon[2627], alsook de oorlog van de VS en Israël tegen Iran.

Artificiële intelligentie en andere datagedreven technologieën spelen een cruciale rol in deze conflicten. Bijgevolg vindt in toenemende mate een militarisering van technologie plaats. Voor Kif Kif is het duidelijk dat deze militarisering een fundamentele bedreiging vormt voor de mensenrechten, waaronder een toename in racisme en discriminatie, ook binnen België. Onderzoek toont namelijk aan dat bij de militarisering van technologie buiten de landsgrenzen een spill-over effect plaatsvindt binnen de landsgrenzen, en dat dit een gevaar vormt voor de democratie[28], onder andere door het gebruik van militaire technologie binnen de politie[29]. In deze sectie analyseren we de impact van de omzetting van militaire datagedreven technologie naar de civiele ruimte, alsook de omzetting van civiele datagedreven technologie naar de militaire ruimte.

---

[24] Amnesty International. (2026, Januari 5). *Russias aggression in Ukraine - Amnesty International*. https://www.amnesty.org/en/projects/russias-aggression-in-ukraine/

[25]Human Rights Council. (2025). Legal analysis of the conduct of Israel in Gaza pursuant to the Convention on the Prevention and Punishment of the Crime of Genocide. In *Conference room paper of the Independent International Commission of Inquiry on the Occupied Palestinian Territory, including East Jerusalem, and Israel*. https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session60/advance-version/a-hrc-60-crp-3.pdf

[26]Israel's Displacement of Civilians in Lebanon is a Possible War Crime. (2026, Maart 26). *Human Rights Watch*. https://www.hrw.org/news/2026/03/23/israels-displacement-of-civilians-in-lebanon-is-a-possible-war-crime

[27] Christou, W. (2026, Augustus 6). Israeli strike that killed journalist in Lebanon was war crime, say rights groups. *The Guardian*. https://www.theguardian.com/world/2026/aug/06/israeli-strike-that-killed-journalist-in-lebanon-was-war-say-rights-groups

[28] Ams, S. (2026). Blurred Lines: How Converging of Military and Civilian Uses of AI & Data May Threaten Liberal Democracy. In: Patton Rogers, J., Hutto, J.W. (eds) Rethinking Remote Warfare. Palgrave Studies in International Relations. Palgrave Macmillan, Cham.

[29]Admin, B., & Admin, B. (2018, Juli 10). Evidence suggests the militarization of police forces leads to more civilian deaths. LSE United States Politics and Policy. https://blogs.lse.ac.uk/usappblog/2018/07/05/evidence-suggests-the-militarization-of-police-forces-leads-to-more-civilian-deaths/

Van militaire naar civiele technologie

Veel gemilitariseerde technologie wordt vandaag ontwikkeld, getest en ingezet in zones waar systematische mensenrechtenschendingen plaatsvinden, zoals oorlogsgebieden, gekoloniseerde gebieden of grensgebieden. Belangrijke voorbeelden zijn technologieën die ontwikkeld of toegepast zijn in de context van bezetting en genocide[30] in Palestina, technologieën die zijn toegepast in de context van misdaden tegen de mensheid op de Oeigoeren in China[31], of in de context van structurele mensenrechtenschendingen aan de buitengrenzen van de Europese Unie[32]. Grenscontroles zijn immers vrijgesteld van veel beschermingen en transparantieverplichtingen die gelden in de rest van Europa; er is zelfs sprake van een parallel wettelijk kader[33]. In België worden alvast verschillende van dergelijke technologieën gebruikt:

- **Cellebrite** is een vorm van spyware die digitale toestellen kan kraken en de inhoud kan lezen. De software werd getest tijdens illegale invallen bij Palestijnen, waarbij hun smartphone in beslag werd genomen en hun data onrechtmatig werd verkregen[34]. Bovendien wordt deze software over heel de wereld gebruikt om mensenrechtenverdedigers te bespioneren en te vervolgen[35], zoals in Rusland, Jemen en Hong Kong[36]. Cellebrite wordt momenteel gebruikt door politiezones verspreid over heel België[37].
- **BriefCam** wordt gebruikt in bezette Palestijnse gebieden door het Israëlische leger en houdt mee de illegale bezetting in stand[38]. De kans is zeer groot dat de algoritmes getraind worden met persoonlijke data van Palestijnen die onrechtmatig zijn verkregen.

---

[30]Loewenstein, A. (2023). The Palestine laboratory: *How Israel exports the technology of occupation around the world*. Verso Books.

[31]Hurry, D. (2025, September 15). *Silicon Valley enabled brutal mass detention and surveillance in China, internal documents show*. The Associated Press. https://www.ap.org/news-highlights/spotlights/2025/silicon-valley-enabled-brutal-mass-detention-and-surveillance-in-china-internal-documents-show/

[32]*Greece a testing ground for smart surveillance technologies*. (2025, November 29). Solomon. https://wearesolomon.com/en/mag/format/investigation/greece-a-testing-ground-for-smart-surveillance-technologies/

[33]hBouvier, C. (2024, April 4). *A dangerous precedent: how the EU AI Act fails migrants and people on the move*. PICUM. https://picum.org/blog/a-dangerous-precedent-how-the-eu-ai-act-fails-migrants-and-people-on-the-move/

[34] American Friends Service Committee. (n.d.). *Companies profiting from the Gaza genocide.* afsc.org

[35] The Citizen Lab. (2026, Mei 14). *From protest to peril: Cellebrite used against Jordanian civil society.* https://citizenlab.ca/research/from-protest-to-peril-cellebrite-used-against-jordanian-civil-society/

[36]Vanhoutte, T. (2025, Augustus 8). Liga voor Mensenrechten en SOS Gaza klagen Israëlische spionagetechnologie bij Vlaamse politiezones aan. *VRTNWS*. https://www.vrt.be/vrtnws/nl/2025/08/08/vlaanderen-gebruikt-technologie-van-israelische-leger/

[37] Van Cauwenberge, D. (2025, Juli 25). *Bijna de helft van alle Vlaamse politiezones gebruikt Israëlische spyware*. https://apache.be/2025/07/25/bijna-helft-van-alle-vlaamse-politiezones-gebruikt-israelische-spyware

[38] *Briefcam*. (n.d.). Who Profits. https://www.whoprofits.org/companies/company/6672

BriefCam werd gebruikt in Hongarije om deelnemers aan de Pride-parade op te sporen[39]. Ook BriefCam wordt momenteel gebruikt door verschillende politiezones in België[40].

Men kan de komst van Palantir naar België in dezelfde context beschouwen. Palantir is een softwarebedrijf in de defensie-industrie dat gespecialiseerd is in datamanagement. Palantir heeft onder andere samengewerkt met de Amerikaanse veiligheidsdienst ICE om mensen zonder papieren op te sporen, en met de Israëlische veiligheidsdiensten tijdens de genocide in Gaza. Palantir maakte ook de overstap naar civiele toepassingen, zoals in de samenwerking met de nationale gezondheidsdienst in Engeland[41]. Palantirs samenwerking met publieke instellingen stuit op brede weerstand van de Europese bevolking en politici[42].

De toenemende invloed van dergelijke techbedrijven is politiek relevant. Deze bedrijven wegen steeds meer door op het beleid, niet alleen in defensie maar ook in domeinen zoals de openbare orde, veiligheid, migratie en gezondheidszorg. De verspreiding van deze technologieën zorgt ook voor de verspreiding van de politieke visie die deze technologie vormgeeft. Deze visie kan het best omschreven worden als volgt: men is de onderdrukker of de onderdrukte (het is eten of gegeten worden) op het wereldtoneel, en voor minderheden, migranten en mensenrechten is er geen plaats[43].

De toepassing van gemilitariseerde technologieën binnen de civiele ruimte brengt verschillende risico's met zich mee:

1. Verzwakking van democratie en en rechtsstaat

De aankoop van deze technologieën beloont en versterkt bedrijven en regimes die mensenrechten systematisch schenden en racistische ideologieën aanhangen. Zo dragen ze bij aan een verzwakking van de democratie en de rechtsstaat.

---

[39] Vanhoutte, T. (2025, Augustus 8). Liga voor Mensenrechten en SOS Gaza klagen Israëlische spionagetechnologie bij Vlaamse politiezones aan. *VRTNWS*. https://www.vrt.be/vrtnws/nl/2025/08/08/vlaanderen-gebruikt-technologie-van-israelische-leger/

[40] Van Cauwenberge, D. (2025, Juli 25). *Bijna de helft van alle Vlaamse politiezones gebruikt Israëlische spyware*. https://apache.be/2025/07/25/bijna-helft-van-alle-vlaamse-politiezones-gebruikt-israelische-spyware

[41] Medact. (2026, Maart 12). *Briefing: Concerns regarding Palantir Technologies and NHS Data Systems*. https://www.medact.org/2026/resources/briefings/briefing-palantir-fdp/

[42] Booth, R. (2026, April 27). Sadiq Khan may try to stop Scotland Yard signing Palantir contract. *The Guardian*. https://www.theguardian.com/politics/2026/apr/27/sadiq-khan-may-try-to-stop-scotland-yard-signing-palantir-contract

[43] Vandenborght, R. (2026, April 30). *De architecten van algoritmische oorlogsvoering*. Visie. https://visie.net/de-gids-artikel/de-architecten-van-algoritmische-oorlogsvoering

2. Juridische aansprakelijkheid

Volgens de Genocideconventie, waarbij alle EU-lidstaten verdragspartij zijn, heeft elk land een juridische verplichting om alle mogelijke maatregelen te nemen om genocide te voorkomen. Landen die weigeren om actie te ondernemen, inclusief een weigering van het stopzetten van handelsrelaties die mogelijks bijdragen aan de uitvoering van een genocide, stellen zich bloot aan juridische procedures[44] [45].

3. Risico op schending fundamentele mensenrechten

Gemilitariseerde technologie is ontwikkeld in een zeer specifieke context, met andere regels, waarden en doelen dan die van de civiele context. De vervaging van de grens tussen de militaire en civiele ruimte brengt fundamentele mensenrechten, zoals het recht op protest en het recht op privacy, in gevaar. Gemarginaliseerde groepen ondervinden daar de grootste gevolgen van[46].

4. Afhankelijkheid van verkoper en datamisbruik

Veel technologische producten steunen op actieve dataverzameling en -verwerking. Producten van deze aard zijn zelden beperkt tot één aankoop, gezien de nood aan voortdurend onderhoud en bijwerking. Toegang tot gevoelige gegevens is vaak noodzakelijk. Dit zorgt voor een afhankelijkheid van de verkoper ('vendor lock-in') en voor risico's op datamisbruik.

Daarom formuleert Kif Kif de volgende aanbevelingen:

---

[44] Vidal, K. (2025, June 20). 18 experts waarschuwen De Wever: "Als België niet alles doet om een genocide te vermijden, dreigt het Internationaal Gerechtshof." *De Standaard*. https://www.standaard.be/buitenland/18-experts-waarschuwen-de-wever-als-belgie-niet-alles-doet-om-een-genocide-te-vermijden-dreigt-het-internationaal-gerechtshof/72932451.html

[45] Pietropaoli, I. (2024). Obligations of Third States and Corporations to Prevent and Punish Genocide in Gaza. In *Somo*. https://www.somo.nl/wp-content/uploads/2024/06/Obligations-of-Third-States-and-Corporations-to-Prevent-and-Punish-Genocide-in-Gaza-3.pdf

[46] Amnesty International. (2025, Augustus 21). *Tech made by Palantir and Babel Street pose surveillance threats to pro-Palestine student protestors & migrants*. https://www.amnesty.org/en/latest/news/2025/08/usa-global-tech-made-by-palantir-and-babel-street-pose-surveillance-threats-to-pro-palestine-student-protestors-migrants/

1. Stap over van bestaande contracten met Israëlische bedrijven

Maak de overstap van reeds bestaande contracten met Israëlische militaire technologiebedrijven, zowel binnen militaire als civiele toepassingen, naar nieuwe contracten een prioriteit. Dit is in lijn met het Palestina-akkoord dat de regering overeenkwam in september 2025. Wees daarbij transparant over de criteria die worden gehanteerd om alternatieven te beoordelen. Stap definitief af van technologieën die een significant risico vormen voor democratische grondrechten.

2. Voer een analyse uit van de impact op mensenrechten voorafgaand aan de aankoop van militaire technologie voor civiele ruimtes

Voer een grondige analyse uit van de mensenrechtenimpact alvorens technologie uit een gemilitariseerde context aan te kopen en in te zetten voor civiele doeleinden, inclusief bij het overstappen van oude naar nieuwe contracten. Zorg daarbij voor een methodologie die de context waaruit de technologie uit voorkomt analyseert en duidelijk onderscheid en vergelijkt met de civiele context waarin deze zou worden toegepast, en diens geschiktheid evalueert. Sluit technologieën die een significant risico vormen voor democratische grondrechten uit. Kif Kif verwijst bijvoorbeeld naar het onderzoek van digitale rechtenorganisatie EDRi, die Cellebrite en gelijkaardige software als spyware bestempelt en oproept tot een verbod van dergelijke software[47].

3. Sluit bedrijven die mensenrechten schenden uit van publieke contracten

Werk een beleidskader uit om bedrijven die betrokken zijn bij ernstige schendingen van het internationaal recht en mensenrechten, uit te sluiten van overheidsopdrachten en publieke aankopen, inclusief in het domein van binnenlandse veiligheid en defensie. Ondersteun daarbij ook lokale en regionale overheden om dit beleidskader toe te passen.

[47]Ajanovic, A. (2025). Spyware and state abuse: The case for an EU-wide ban. In *European Digital Rights (EDRi)*. https://edri.org/wp-content/uploads/2025/06/EDRi_Spyware-position-paper.pdf

4. Zorg dat computercode die ontwikkeld is met publieke middelen eigendom blijft van de overheid

Zorg dat computercode die ontwikkeld is voor de overheid en aangekocht is met publiek geld, eigendom blijft van de overheid, om zo de veiligheid van data en digitale infrastructuur te waarborgen.

5. Weer Palantir uit overheidsopdrachten

Weer Palantir bij voorbaat uit overheidsopdrachten en publieke aankopen. De waarden van dit bedrijf zijn niet alleen rechtstreeks onverenigbaar met de democratie en mensenrechten. Ze vormen ook een gevaar voor de veiligheid van de data van Belgische burgers en riskeren de Europese autonomie in gevaar te brengen, gezien Palantirs verstrengeling met de overheid van de Verenigde Staten. Dit risico is erkend door onder andere het Zwitserse leger[48]. Deze aanbeveling is in lijn met de doelstellingen inzake soevereiniteit van de Europese Cloud and AI Development Act.

6. Voorzie een volledig verbod op biometrische massasurveillance en voorspellend profileren

De AI Act laat op gevaarlijke wijze de deur openstaan voor het gebruik van biometrische massasurveillance en voorspellend profileren door de politie- en andere veiligheidsdiensten in bepaalde gevallen. Deze technologie brengt een hoog risico op discriminatie met zich mee. Onderzoek[49] toont namelijk aan dat de meest gemarginaliseerde groepen in onze samenleving systematisch meer kans hebben om door deze technologieën benadeeld te worden. Herkenningssystemen zullen mensen van kleur bijvoorbeeld vaker foutief identificeren. Het verbeteren van de foutmarges is echter geen oplossing. Verschillende gemeenschappen van mensen van kleur hebben immers historisch gezien te maken gehad met overmatige politiesurveillance, en de technologieën die zich baseren op historische data zouden deze tendens versterken, met systematische mensenrechtenschendingen tot gevolg. België kan een voortrekkersrol opnemen in Europa door een verbod in te voeren.

[48] Fichter, A., Meyer, M., Naegeli, L., Steiner, J. (2026, Februari 18). *How tenaciously Palantir courted Switzerland*. Republik. republik.ch

[49] Williams, P., & Kind, E. (2019). Data-driven policing. The hardwiring of discriminatory policing practices across Europe. https://www.enar-eu.org/wp-content/uploads/data-driven-profiling-web-final.pdf

Militarisering van civiele technologie

Datagedreven technologie ontwikkeld binnen de civiele ruimte wordt ook steeds meer toegepast voor militaire doeleinden. Een voorbeeld daarvan is het gebruik van de AI-software Claude door de VS in de oorlog tegen Iran[50].

Deze militarisering van civiele technologie vindt plaats binnen de context van de race om AI-dominantie van staten en bedrijven, alsook de geopolitieke spanningen en verregaande militarisering. De huidige internationale verdragen en rechtsmechanismen volstaan niet om ervoor te zorgen dat die datagedreven oorlogssystemen het internationaal humanitair recht en de mensenrechten respecteren[51]. Uitdagingen omvatten onder andere ontmenselijking door de reductie van mensen tot datapunten, het voortzetten van algoritmische bias, stereotypering en discriminatie op basis van gender, etniciteit en andere sociale identiteiten, afwezigheid van menselijke besluitvorming, transparantie en aansprakelijkheid, het verkorten van de 'kill-chain' (de tijd die nodig is tussen het identificeren van een doelwit en het uitvoeren van een dodelijke actie), de onbetrouwbaarheid van geautomatiseerde besluitvorming, en het normaliseren en faciliteren van oorlogsdaden en -misdaden, die voornamelijk het Globale Zuiden en gemarginaleerde gemeenschappen treffen[52].

De militarisering van civiele technologie zorgt niet alleen voor uitdagingen in oorlogs- en conflictzones, maar ook binnen België. AI-toepassingen zijn op het gebied van nationale veiligheid nog grotendeels ongereguleerd, en ook de term ‘nationale veiligheid’ is niet duidelijk gedefinieerd. De ruime uitzonderingen en vrijstellingen voor nationale veiligheid in de bestaande AI-wetgeving, waaronder artikel 2 van de EU AI Act en artikel 3, lid 2, van het Kaderverdrag van de Raad van Europa inzake AI en mensenrechten, de rechtsstaat en democratie, hebben geleid tot aanzienlijke lacunes in de regelgeving[53].

Het gebrek aan wettelijk kader, zowel op Europees als nationaal niveau, inzake AI in de context van nationale veiligheid betekent dat AI riskeert ontwikkeld, getest en toegepast te worden zonder de juiste waarborgen voor de mensenrechten, zeker binnen de huidige politieke context.

---

[50]Chandran, R. (2026, Maart 5). Black-box AI and cheap drones are outpacing global rules of war. *Rest of World*. https://restofworld.org/2026/anthropic-ai-and-iran-drone-warfare/
[51] Denise Garcia (2024) Algorithms and Decision-Making in Military Artificial Intelligence, Global Society, 38:1, 24-33.
[52]Access Now. (2026, Juni 15). *Joint statement on AI in warfare*. https://www.accessnow.org/press-release/joint-statement-on-ai-in-warfare/
[53]Harrison, A. S., & Wisniak, M. (2026). Automating Repression Beyond Borders: How AI is Powering Transnational Repression. In *ECNL*. https://ecnl.org/sites/default/files/2026-03/ECNL%20Digital%20Transnational%20Repression%20AI_1.pdf

Dit risico is ook erkend door het Vlaamse kenniscentrum Data en Maatschappij, in een analyse van de Vlaamse Innovatie- en Industriestrategie voor Veiligheid en Defensie (VISD) en de bijbehorende roadmaps: *'Deze civiel-naar-militair-richting is bestuurlijk relevant. Ze betekent dat technologieën die ontwikkeld worden onder civiele reguleringskaders, waaronder de EU AI Act, doelbewust worden gekanaliseerd naar militaire toepassingen die van datzelfde kader zijn vrijgesteld. De strategiedocumenten gaan niet in op hoe deze overgang wordt bestuurd, welk toezicht geldt op het moment van omzetting, of welke waarborgen meereizen met de technologie van civiele oorsprong naar militaire toepassing.'* [54] Daarbij werd ook een gebrek aan een duidelijk ethisch kader opgemerkt, alsook een gebrek aan regels inzake aansprakelijkheid bij schade van AI-systemen afkomstig uit civiele context met militaire toepassing.

Bijgevolg formuleert Kif Kif de volgende aanbevelingen:

1. Ontwikkel een juridisch kader rond AI en datagedreven technologieën bij de omzet van civiele naar militaire toepassingen.

Ontwikkel een duidelijk juridisch kader dat de ontwikkeling en inzet van AI en andere data-gedreven technologieën binnen militaire toepassingen en het domein van nationale veiligheid reguleert. Zorg daarbij dat het juridisch kader de overgang van technologie van de civiele naar militaire context reguleert, waarbij civiele data beschermd zijn.

2. Stel mensenrechten voorop in het juridische kader

Besteed ruime aandacht aan bescherming van de mensenrechten conform het internationaal humanitair recht en mensenrechtenverdragen binnen dit juridisch kader. Dit omvat onder andere de nood aan verregaand menselijk toezicht, duidelijke aansprakelijkheidsregels en procedures voor mensen die schade hebben ondervonden en transparantie over naar het publiek toe over hoe technologieën worden ingezet.

3. Verbied AI-gedreven militaire doelwitherkenning

[54] Heymans, F. (2026, March 19). *Vlaanderen - Impulsprogramma Defensie: AI en autonome technologie*. Data En Maatschappij. https://data-en-maatschappij.ai/publicaties/vlaanderen-impulsprogramma-defensie-ori%C3%ABntatieroadmap-ai-for-defence

In navolging van meer dan tweehonderd middenveldorganisaties en particulieren[55]: verbied het gebruik van AI-gedreven militaire doelwitherkenning wegens de fundamentele incompatibiliteit met het internationaal recht, de mensenrechten en menselijke waardigheid.

[55]Access Now. (2026, Juni 15). *Joint statement on AI in warfare*. https://www.accessnow.org/press-release/joint-statement-on-ai-in-warfare/

5. Big Tech en een rechtvaardige digitale wereld

Digitale infrastructuur en diensten hebben in de moderne samenleving een grote invloed op hoe de samenleving georganiseerd wordt. De toegang tot markten, tot bankdiensten, tot het publieke debat en nog veel andere domeinen wordt telkens in grote mate bepaald door digitale technologieën. Inclusieve, duurzame en rechtvaardige digitale technologieën zijn dus essentieel voor een inclusieve, duurzame en rechtvaardige samenleving.

Vandaag de dag is de digitale wereld echter grotendeels in handen van enkele grote, voornamelijk Amerikaanse, technologiebedrijven, ook wel bekend als Big Tech. Daaronder rekenen we onder andere Microsoft, Google/Alphabet, Amazon, Meta, Apple, X en OpenAI. De enorme concentratie van macht en rijkdom in dit kleine aantal bedrijven is een bedreiging voor de democratie en mensenrechten. Zoals uitvoerig beschreven in dit document, zijn daarbij telkens gemarginaliseerde groepen die op verschillende manieren het sterkst getroffen worden door de nadelige effecten van de macht van deze techbedrijven.

Daarbij komt ook de impact van de activiteiten van Big Tech op het milieu en het klimaat. AI verbruikt bijvoorbeeld enorme hoeveelheden water en energie. Dit verhoogt de afhankelijkheid van fossiele brandstoffen die nefast zijn voor het klimaat, en versterkt de reeds bestaande permanente waterschaarste[56][57]. Datacenters brengen dan ook stijgende energieprijzen, droogte en vervuiling met zich mee. De negatieve gevolgen worden ongelijk verdeeld en treffen gemarginaliseerde groepen het sterkst.

Om dit probleem structureel aan te pakken moet er een tweeledige beleidsstrategie zijn. Enerzijds moet men de marktmacht van deze monopolistische bedrijven aanpakken, om hun macht te beperken en competitie aan te moedigen. Anderzijds moet men nieuwe, rechtvaardigere en ecologische alternatieven ondersteunen. Zo kan men tot een gezonder digitaal ecosysteem komen.

De huidige aandacht binnen de Europese Unie aan soevereiniteit en digitale onafhankelijkheid, met name met de Tech Sovereignty Package, bieden een kans om een democratische digitale wereld op te bouwen die iedereen tegemoetkomt. Het doel is echter niet om een Europese Big

[56] Gröger, J., Behrens, F., Gailhofer, P., & Hilbert, I. (n.d.). Environmental impacts of artificial intelligence. In *Greenpeace*. https://www.greenpeace.de/publikationen/20250514-greenpeace-studie-umweltauswirkungen-ki-eng.pdf

[57] *World enters era of 'global water bankruptcy.'* (2026, Januari 20). UN News. https://news.un.org/en/story/2026/01/1166800

Tech-industrie te creëren maar om een volwaardig open, democratisch, duurzaam en publiek alternatief op te bouwen. Hiervoor moet men zowel op federaal als Europees niveau beleidsmaatregelen nemen. We bevelen dan ook het volgende aan:

1. Dwing de wetgeving tegen monopolievorming in de digitale sector af

Zorg voor een strengere handhaving en betere opvolging, implementatie en evaluatie van de verschillende wetgevende kaders tegen monopolievorming in de digitale sector. Dit geldt voor de Belgische wetgeving[58], maar ook voor de Europese wetgeving[59]. Hoewel de Europese wetgeving door de Commissie wordt afgedwongen, vragen we om op Europees niveau maatregelen aan te moedigen om de handhaving van de wetgeving te versterken en de wetgeving uit te breiden, zoals generatieve AI onder de Digital Markets Act te laten vallen.[60] Voorkom verdere machtsconcentratie door fusies en overnames.

2. Stap zo snel mogelijk af van de diensten van Big Tech binnen overheidsdiensten

Een groot deel van de afhankelijkheid van Big Tech is afkomstig uit digitale ecosystemen die een groot aantal functies integreren binnen één dienst, zoals servercapaciteit dataopslag, data-analyse, online collaboratietools, etc.[61] Onderzoek toont aan dat in België meer dan 70% van lokale Belgische gemeenten Microsoft gebruiken[62]. Gebruik de Europese Open Source Strategy als opportuniteit om binnen Belgische overheidsdiensten zo spoedig mogelijk af te stappen van Big Tech.

3. Wedijver op Europees niveau voor aanpassingen aan de Cloud and AI Development Act

---

[58] Federale Overheidsdienst Economie, KMO's, Middenstand en Energie. (2024). Belgische markt voor online platformen: Evaluatie van de mededinging en het regelgevend kader – Samenvatting.

[59] Penfrat, J. (2023, Augustus 2). *Regulating Big Tech in Europe with the Digital Services Act & Digital Markets Act*. European Digital Rights (EDRi). https://edri.org/our-work/regulating-big-tech-in-europe-with-the-digital-services-act-digital-markets-act/

[60] *The DMA is a success, it should be strengthened and expanded*. (2025, Oktober 16). European Digital Rights (EDRi). https://edri.org/our-work/the-dma-is-a-success-it-should-be-strengthened-and-expanded/

[61] ARTICLE 19. (n.d.). *Response to the European Commission Call for Evidence Cloud and AI Development Act (CADA)*. https://www.article19.org/wp-content/uploads/2026/06/20260304_ARTICLE19_CADA_condensed.pdf

[62] Gaeremyn, J. (2025, Maart 8). European critical dependencies. *Pseudo Random Noise*. https://jurgen.gaeremyn.be/2025/03/08/european-critical-dependencies/

Vraag op Europees niveau aanpassingen aan de Cloud and AI Development Act (CADA) in functie van een digitale infrastructuur voor het publieke goed, in plaats van onnodig te participeren in een globale AI-wedloop. CADA gaat er onterecht van uit dat een massale uitbreiding van Europa's servercapaciteit nodig is[63]. Deze uitbreiding en investering is onverenigbaar met sociale en ecologische doelstellingen[64]. Neem in plaats daarvan maatregelen om de bestaande cloudinfrastructuur, met name infrastructuur die frontier AI modellen (geavanceerde AI-modellen die bovengemiddeld veel rekenkracht vergen) aandrijft, uit de handen te nemen van Amerikaanse hyperscalers (grote cloudproviders). Men kan bijvoorbeeld transparantievereisten opleggen aan cloud providers en een meer flexibele Europese marktplaats voor cloudinfrastructuur[65] uitbouwen. Maak naast de soevereiniteitsimpactanalyse ook mensenrechtenimpactanalyses verplicht bij de beoordeling van cloud providers. Vraag op Europees niveau een grondig debat en analyse over de reële digitale noden, dat technologische doelstellingen balanceert met sociale en ecologische doelstellingen.

4. Belast dominante techbedrijven in België

Leg belastingen op aan dominante techbedrijven in België waarbij men belast op basis van de locatie waar de digitale activiteiten plaatsvinden en investeer de opbrengsten in publieke alternatieven[66]. Zo wordt oneerlijke concurrentie ingeperkt en kan de digitale sector vernieuwen.

5. Investeer in onderzoek naar alternatieve technologieën

Investeer in onderzoek en ontwikkeling van AI en datagedreven technologieën die verenigbaar zijn met de sociale en ecologische doelstellingen om zo de afhankelijkheid van Big Tech op lange termijn te verminderen.

---

[63]Von Thun, M. (2026, Juni 16). Europe is starting to break up with US big tech. But it's still abiding by the Silicon Valley rulebook. *The Guardian*. https://www.theguardian.com/commentisfree/2026/jun/15/europe-us-big-tech-silicon-valley-european-commission

[64]Thorne, M., Delgado, A. G., Jansen, F., & Leonard, R. (2026, Juli 28). *The case for a temporary moratorium on large data centers in Europe*. Tech Policy Press. https://www.techpolicy.press/the-case-for-a-temporary-moratorium-on-large-data-centers-in-europe/

[65]ARTICLE 19. (n.d.). *Response to the European Commission Call for Evidence Cloud and AI Development Act (CADA)*. https://www.article19.org/wp-content/uploads/2026/06/20260304_ARTICLE19_CADA_condensed.pdf

[66] Balanced Economy Project et al. (2024). *Beyond Big Tech: A framework for building a new and fair digital economy*.

Conclusie

Digitaal racisme kent vele vormen en uit zich op verschillende niveaus. Allereerst op niveau van de technologie zelf, zoals bij bias in AI of algoritmes op sociale media die haatdragende content aanmoedigen om het engagement te maximaliseren. Het uit zich ook op niveau van het *gebruik* van technologie, zoals contentmoderatie (of het gebrek daaraan) op sociale media, of het gebruik van gemilitariseerde technologie die fundamentele mensenrechten bedreigt. Tot slot uit digitaal racisme zich ook binnen de bredere maatschappelijke en institutionele context, bijvoorbeeld in de plaatsing van datacentra in armere gemeenschappen, of het schadelijke businessmodel van Big Tech.

Big Tech-bedrijven monopoliseren de markt en vergaren een ongekende hoeveelheid macht en rijkdom, waardoor aansprakelijkheid en democratische controle steeds moeilijker worden. Tegelijkertijd bevinden we ons in een politieke context gekenmerkt door geopolitieke spanningen en de vraag vanuit bedrijven en bepaalde politieke partijen om te dereguleren.

In deze uitdagende context is sterk en doortastend beleid cruciaal. Bestaande wetten op Europees niveau, zoals de DSA en DMA, bieden effectieve beleidsinstrumenten om digitaal racisme tegen te gaan. De uitdaging bestaat erin om de strikte handhaving van deze wet een politieke prioriteit te maken. Ook moet het een prioriteit zijn om pogingen om bestaande en toekomstige wetgeving uit te hollen, tegen te houden, zoals de Data Omnibus. Daarnaast moet er waakzaam worden opgetreden in de nieuwe Cloud and AI Development Act en gevraagd worden om aanpassingen. Het uitbreiden van de capaciteit van Europese datacentra is niet alleen sociaal en ecologisch schadelijk, het zal ook niet bijdragen aan Europese digitale soevereiniteit.

Dit betekent niet dat er geen doeltreffende maatregelen op Belgisch en federaal niveau kunnen genomen worden. België kan de lacunes in Europese wetgeving aanvullen, bijvoorbeeld door een verplicht transparantieregister in te voeren voor AI-systemen die Belgische overheden gebruiken. Deze maatregel zou helpen bij het opsporen van digitale discriminatie en racisme. Ook een verbod op biometrische massasurveillance en het creëren van een duidelijk wettelijk kader dat mensenrechten vooropstelt inzake het gebruik van civiele AI voor militaire toepassingen, en vice versa, zou een zeer grote stap in de goede richting zijn.

Tot slot blijven we aansporen om systematisch het middenveld te versterken, en te betrekken bij onderzoek en samenwerkingen in bepaalde onderwerpen waar kennis nog steeds ontbreekt.

Indien deze maatregelen gevolgd worden, kan digitaal racisme op een structureel niveau aangepakt worden, om een veilige en inclusieve digitale ruimte te creëren. Kif Kif biedt zich graag aan als constructieve partner in dit proces.