Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

32 761 Verwerking en bescherming persoonsgegevens

Nr. 262

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 februari 2023

Bij brief van 18 november 2022 heb ik u onder meer geïnformeerd over de resultaten van een Data Protection Impact Assessment (DPIA) en een Human Rights Impact Assessment (HRIA) die ik heb laten uitvoeren op het gebruik van Facebookpagina's door de overheid.[1]

Ik heb u daarbij ook een vertaling hiervan toegezegd. De vertalingen van beide assessments zijn als bijlagen bij deze brief gevoegd. Hierbij is gekozen voor een begrijpelijke Nederlandstalige samenvatting, omdat beide documenten een sterk technisch karakter kennen. Ik vind het gezien het belang van het onderwerp namelijk belangrijk dat de inhoud van de documenten voor een breed publiek begrijpelijk is.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen

[1] Kamerstuk 32 761, nr. 252.

kst-32761-262
ISSN 0921 - 7371
's-Gravenhage 2023

Bijlage

Nederlandstalige samenvatting Data Protection Impact Assessment

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft onderzoek laten doen door Privacy Company naar de privacyrisico's voor mensen van het gebruik van Facebook-pagina's door de Nederlandse overheid. Zo'n onderzoek heet een gegevensbeschermingseffectbeoordeling, in het Engels: een Data Protection Impact Assessment, oftewel DPIA. Deze DPIA wordt gecombineerd met een afzonderlijke mensenrechteneffectbeoordeling (HRIA), over de risico's voor het recht van mensen op non-discriminatie, vrijheid van gedachte, geweten en godsdienst, en vrijheid van meningsuiting en informatie.

Facebook/Meta

In januari 2022 veranderde Facebook zijn bedrijfsnaam in Meta Platform Inc. Het onderzoeksrapport gebruikt toch nog de naam «Facebook» voor het sociale media platform, om verwarring te voorkomen met andere apps die Meta aanbiedt, zoals Instagram en WhatsApp.

Iedereen met een Facebook-account kan een Facebook-pagina aanmaken om contactgegevens te delen, updates te plaatsen, nieuwsberichten te delen en te communiceren met een publiek van vrienden of een groter onbekend publiek. Vroeger stonden Facebook-pagina's voor organisaties bekend als *Fan Pages*. Er is geen aparte naam meer voor pagina's die zijn aangemaakt door bedrijven, merken, organisaties en publieke figuren.

Facebook-gebruikers die een pagina leuk vinden of volgen, krijgen updates van die organisatie in hun Nieuwsfeed. De Nieuwsfeed is een dynamische lijst van inhoud op de Facebook-homepage van elke gebruiker met statusupdates, foto's, (live) video's, links, app-activiteit en likes van mensen, Pagina's en groepen. De inhoud wordt beïnvloed door de activiteiten en likes van vrienden.

Waar gaat de DPIA over?

De DPIA gaat over het genereren en gebruiken van website analytics (de Insights uit de Meta Business Suite) en andere gegevens die Facebook bijhoudt over het gedrag van bezoekers op een Page. Facebook stelt statistieken beschikbaar aan de eigenaar van de Facebook-pagina.

Deze DPIA beoordeelt het privacyrisico van de gegevensverwerking door Facebook als gevolg van bezoek aan een overheidspagina. Deze verwerking bestaat bijvoorbeeld uit het tonen van individuele aanbevelingen aan bezoekers van de Facebook-testpagina, en aanbevelingen in de News Feed van de bezoekers als gevolg van hun gedrag: als ze klikken op aanbevolen artikelen of hyperlinks.

Omdat Facebook niet de mogelijkheid biedt om werkaccounts aan te maken, gebeurt het aanmaken en onderhouden van Facebook-pagina's van overheidsorganisaties vaak met de privé Facebook accounts van medewerkers van die organisaties. Daarom beoordeelt deze DPIA ook de risico's voor werknemers bij het onderhouden van een Facebook-pagina.

Deze DPIA geeft ook een beoordeling van de juridische (niet technische) risico's van onrechtmatige toegang door Amerikaanse overheidsinstanties tot persoonsgegevens die door Facebook worden verwerkt als gevolg van het gebruik van een overheidspagina.

Hoe is er getest?

Voor deze DPIA is een testpagina aangemaakt, van een niet-bestaande overheidsinstelling (het Ministerie van Privacy). Er zijn ook twee nieuwe persoonlijke Facebook-accounts gemaakt. Een maand lang bezochten de twee testers elke dag de overheidstestpagina. Een bestaande Facebook-gebruiker trad op als beheerder van de pagina en communiceerde met de twee nieuwe accounts. De twee nieuwe accounts «bevrienden» niemand anders dan elkaar (op een paar uitzonderingen na), maar deden verschillende dingen op Facebook. Het ene account volgde alle Nederlandse politieke partijleiders uit de Tweede Kamer en vond hun posts (lukraak) leuk, evenals twee Ministeries (BZK en OCW) en drie publieke instellingen (RIVM, ProDemos en KNMI). Het andere account raakte bevriend met publieke LGBTI-personen en het Ministerie van Defensie en vond hun posts ook leuk. Wanneer het volgen van pagina's leidde tot aanbevelingen voor andere pagina's, werden sommige van deze aanbevelingen opgevolgd, wat weer leidde tot het volgen van andere pagina's. Al het uitgaande netwerkverkeer is onderschept. Elke 5 seconden zijn automatisch schermfoto's gemaakt van de Nieuwsfeed van de twee testaccounts, en van de inhoud van de testpagina. Na afloop van de test hebben de onderzoekers verzoeken ingediend bij de systeembeheerder van de testpagina om inzage in de verzamelde persoonsgegevens. De paginabeheerder heeft die verzoeken doorgestuurd aan Facebook.

Resultaat: 7 hoge en 1 lage privacyrisico's

De uitkomst van deze DPIA is dat er 7 hoge en 1 lage privacyrisico's zijn wanneer overheidsorganisaties een Facebook-pagina gebruiken om met een massapubliek te communiceren. Deze DPIA beveelt een aantal maatregelen aan die Facebook zou kunnen nemen om deze risico's te beperken. Hoewel overheidsorganisaties een paar maatregelen kunnen nemen om sommige risico's gedeeltelijk te beperken, kunnen overheidsmaatregelen niet alle hoge risico's verhelpen. Zelfs als de Europese Commissie en de regering van de Verenigde Staten later in 2023 een nieuwe trans-Atlantische gegevensbeschermingsovereenkomst sluiten, kan de wereldwijde gegevensverwerking door Facebook nog steeds zorgen voor hoge privacyrisico's. Dit omdat persoonsgegevens via Facebook toegankelijk zijn in heel veel landen zonder passende privacywetgeving.

Doelen, rollen en grondslagen

De onafhankelijke onderzoekers beschrijven 15 doelen, met nog aanvullende subdoelen, waarvoor Facebook de persoonsgegevens verwerkt die het bedrijf krijgt door bezoek aan een overheidspagina. Deze doelen zijn bijvoorbeeld profilering en het tonen van gerichte reclame, gedeeltelijk gebaseerd op het gebruik van volgcookies en unieke nummers uit de apparatuur van de pagina-bezoekers.

Facebook biedt alleen een gezamenlijke verantwoordelijkheidsovereenkomst voor het tonen van de statistieken over het paginabezoek (de Insights). Facebook biedt geen overeenkomst aan voor de andere gegevens die zij verwerken als gevolg van bezoek aan een overheidspagina, omdat Facebook vindt dat zij zelfstandig verantwoordelijk zijn. Volgens het onderzoeksrapport is dat onterecht. Volgens de de onderzoekers zijn de overheidsorganisaties en Facebook gezamenlijk verantwoordelijk voor de verwerking van alle persoonsgegevens in verband met bezoek aan een overheidspagina. Zonder overeenkomst, zo stellen zij, heeft de overheid geen grondslag om persoonsgegevens van bezoekers te verstrekken aan Facebook als onafhankelijke derde partij. Facebook heeft

geen grondslag om de bezoekergegevens te verwerken voor allerlei commerciële doelen. Facebook verwerkt gevoelige afgeleide gegevens over het surfgedrag, en krijgt niet de wettelijk vereiste uitdrukkelijke toestemming van pagina-bezoekers. Facebook is niet transparant over de logica van de algoritmes waarmee het bedrijf bezoekers persoonlijke informatie toont, en welke persoonsgegevens het bedrijf afleidt uit websitebezoeken en communicatieacties. Overheidsinstellingen hebben geen knop om de gegevensverwerking van hun paginabezoekers door Facebook voor commerciële doelen uit te zetten. Facebook maakt misleidend gebruik van volgcookies. Technisch gezien kan de verwerking van grootschalige gegevens door Facebook worden beschreven als bewuste onduidelijkheid door ontwerp. [*obscurity by design*].

Een van de doelen waarvoor Facebook gegevens verwerkt, is voldoen aan bevelen van overheidsorganisaties in derde landen zonder passende privacywetgeving, zoals Amerika. Uit de openbare rapporten van Facebook over dergelijke verstrekkingen volgt dat er een reële mogelijkheid bestaat dat persoonsgegevens over bezoeken aan Nederlandse overheidspagina's aan Amerikaanse opsporings- en inlichtingendiensten worden verstrekt.

Risico's en risicobeperkende maatregelen

In de tabel hieronder staan de 7 hoge en 1 lage beschermingsrisico's voor de pagina-bezoekers, met de risicoverlagende maatregelen die de overheidsorganisaties en Facebook volgens het onderzoeksrapport kunnen nemen.

Nr.	Hoog Risico	Maatregelen overheid	Maatregelen Facebook
1.	Onvermogen om rechten van betrokkenen uit te oefenen	Stop het gebruik van Facebook-pagina's totdat Facebook zinvolle inzage biedt in de logica van zijn gegevensverwerking	Zorg voor zinvolle inzage in de logica van de gepersonaliseerde inhoud, inclusief afgeleide informatie en interessevoorspellingen en stel gebruikers in staat om verkeerde gegevens te verwijderen. Bouw zinvolle tooling om een dergelijke inzage te bieden bij elke posting in de Nieuwsfeed
2.	Beperkend effect op het uitoefenen van andere grondrechten	Maak alle informatie ook beschikbaar op openbare webpagina's, buiten het Facebook-platform	Geef doorgelichte onderzoekers toegang tot feitelijke gegevens die Facebook verwerkt met betrekking tot populaire overheidspagina's, om te onderzoeken of het volgen van een overheidspagina leidt tot een toename of afname van verschillende standpunten die in de personalisatie worden weergegeven. Bovendien moeten onderzoekers A/B-tests kunnen uitvoeren in een geïsoleerd lab, met modelaccounts. Momenteel verbiedt Facebook het gebruik van testaccounts.
		Waarschuw pagina-beheerders om inte loggen met een special paginabeheers account nadat de pagina is gemaakt met het privé account.	
3.	Gebrek aan transparantie over doelen van de verwerking	–	Breidt de gezamenlijke verantwoordelijke overeenkomst voor Insights uit naar alle gegevensverwerkingen door bezoek van overheidspagina's, door Facebook-gebruikers en niet-gebruikers, met inbegrip van afgeleide informatie en interessevoorspellingen.
			Stop met het afdwingen van het gebruik van het datr-cookie bij bezoekers zonder Facebook account
			Standaard privacyvriendelijke instellingen gebruiken voor cookies. Gebruik geen misleidend ontwerp.

Nr.	Hoog Risico	Maatregelen overheid	Maatregelen Facebook
4.	Verlies van controle door verdere verwerkingen door Facebook	Als Facebook knoppen bouwt voor dataminimalisatie: gebruik die	Bouw een opt-out voor beheerders van overheidspagina's voor verdere verwerkingen buiten de overeengekomen doelen in de gezamenlijke verantwoordelijkheids overeenkomst
			Stop met het afdwingen van het gebruik van het datr-cookie voor alle paginabezoekers
		Als Facebook een manier bouwt om de gegevensopslag te beperken: kies de kortste bewaartermijn	Bouw een knop voor beheerders van overheidspagina's om de bewaartermijn zelf te bepalen van de ruwe gegevens over paginabezoeken
5.	Verlies van controle door doorgifte van persoonsgegevens met derde partijen	Leg paginabezoekers uit dat ze de cookies uit hun browser moeten weggooien na het paginabezoek	Stop met het afdwingen van het gebruik van het volgcookies
			Verwijder alle Facebook-cookies wanneer een gebruiker uitlogt. Lees alleen de apparaat-ID's/cookies luit als er een authenticatiecookie is dat aangeeft dat de gebruiker is ingelogd
			Krijg uitdrukkelijke, geïnformeerde toestemming voor alle volgcookies, om rekening te houden met de gevoelige aard van informatie over het surfgedrag
			Krijg uitdrukkelijke, geïnformeerde toestemming voor doorgifte van gegevens aan derde partijen.
6.	Verlies van controle, heridentificatie van gepseudonimiseerde gegevens door eventuele verstrekking aan Amerikaanse autoriteiten	Stop met het gebruik van Facebook-pagina's (heroverweeg dat als er een nieuwe trans-Atlantische gegevensovereenkomst is).	Stop met de doorgifte van persoonsgegevens van bezoekers van Nederlandse overheidspagina's aan de VS. Heroverweeg de weigering om een speciale EU-cloud te openen
			Geef gedetailleerde statistieken aan Nederlandse overheidsorganisaties over de verstrekkingen van persoonsgegevens van bezoekers van Nederlandse overheidspagina's
			Bewaar persoonsgegevens over bezoeken aan Nederlandse overheidspagina's niet langer dan 1 week, en maak wekelijks Insights
7.	Filter bubble: gemiste berichten	Nodig paginabezoekers uit om zich te abonneren op een speciale mailinglijst of een ander niet-algoritmisch communicatiekanaal	Voldoe aan artikel 29 van de DSA en biedt gebruikers de mogelijkheid om een niet-gepersonaliseerde Nieuwsfeed te selecteren
			Stel gebruikers in staat zich aan te melden om altijd berichten van een overheidspagina in de top 10 van de Nieuwsfeed te ontvangen

Conclusies

Het onderzoeksrapport concludeert dat overheidsorganisaties moeten stoppen met het gebruik van Facebook-pagina's als Facebook geen maatregelen neemt om de hoge gegevensbeschermingsrisico's te verhelpen. De Nederlandse overheid is in gesprek met Facebook over het wegnemen van de hoge risico's.

Nederlandstalige samenvatting Human Rights Impact Assessment

In opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft Privacy Company een rapport geschreven over de mensenrechtenrisico's van het gebruik van Facebook-pagina's door de Nederlandse overheid. Deze Human Rights Impact Assessment (HRIA) gaat over de risico's die verbonden zijn aan het bezoeken van Facebook-pagina's van de rijksoverheid. Het gaat om risico's voor het recht op non-discriminatie, vrijheid van gedachte, geweten en godsdienst, en vrijheid van meningsuiting en informatie. Deze HRIA moet samen worden gelezen met de beoordeling van de privacyrisico's door het gebruik van Facebook-pagina's in een uitgebreid DPIA-rapport.

Het rapport concludeert dat het gebruik van Facebook-pagina's door Nederlandse overheidsorganisaties een grote impact kan hebben op de mensenrechten. Door het gebrek aan transparantie (waaronder zinvolle

inzage in de grootschalige gegevensverwerkingen bij Facebook) konden de onderzoekers de werkelijke impact niet beoordelen. Facebook gebruikt algoritmen om te bepalen welke soorten berichten ze toont aan mensen die een overheidspagina hebben bezocht. Nederlandse overheidsorganisaties hebben niet de middelen om de algoritmen die Facebook gebruikt te controleren, bij te stellen/te minimaliseren of zelfs maar uit te leggen aan bezoekers.

Door het gebrek aan transparantie en gebrek aan middelen om de mogelijke negatieve gevolgen voor de personen die de overheidspagina's bezoeken tot een minimum te beperken, moeten overheidsorganisaties ervan uitgaan dat het gebruik van Facebook-pagina's leidt tot een hoog risico voor de mensenrechten.

Facebook slaat informatie op over al het gedrag op pagina's, zoals het openen van een bericht, de tijd die iemand besteedt aan het lezen van een bericht, het *leuk vinden* ervan en/of het doorsturen naar een vriend. Wanneer iemand een Nederlandse overheidspagina op Facebook bezoekt, kan dat bezoek invloed hebben op de berichten en advertenties die Facebook toont. Ook maakt Facebook gebruik van algoritmen om de inhoud te selecteren die het bedrijf aan zijn gebruikers presenteert: er is teveel informatie op Facebook. De algoritmen maken daarom selecties van alle updates van vrienden, de vrienden van hun vrienden en van de inhoud van gevolgde Pages.

Deze HRIA beschrijft zes manieren waarop deze algoritmen bevooroordeeld kunnen zijn. Het rapport toont aan dat een van die typen vooroordelen zeker aanwezig is: vertekening door eenzijdige suggesties. Twee andere type vooroordelen zijn zeer waarschijnlijk aanwezig: namelijk vertekening door *feedback loops* (doorlopende terugkoppeling) en vertekening door optimalisatiecriteria.

Dit is aangetoond via de aanbevelingen die Facebook deed tijdens het (beperkte) onderzoek voor deze DPIA en HRIA. De algoritmen van Facebook selecteerden anti-overheidsstandpunten, omdat die de meeste reacties uitlokken met *vind-ik-leuks*. Facebook's keuze om berichten met de meeste *vind-ik-leuks* hoger te waarderen, zorgt sowieso al voor een vooroordeel. Bovendien sturen de algoritmen de gebruiker één kant op (in dit geval, naar meer anti-overheidsstandpunten).

Facebook's keuze voor een algoritme met zo'n *feedback loop* kan het effect versterken, omdat de belangrijkste door Facebook geselecteerde berichten de meeste kans maken op nieuwe kliks en *vind-ik-leuks*.

De algoritmen kunnen gebruikers sturen in de richting van minder diversiteit of vertegenwoordiging van minderheden. Door de voorkeur te geven aan specifieke inhoud, kunnen algoritmes gebruikers in de richting van bepaalde acties, meningen of denkrichtingen duwen, terwijl ze andere groepen discrimineren of buiten beeld brengen.

Facebook heeft in het onderzoek geen informatie gegeven over de gegevens die het bedrijf gebruikt voor zijn algoritmische beslissingen. Facebook heeft ook geen inzicht gegeven in de toegepaste logica in antwoord op de individuele inzageverzoeken. Dit gebrek aan transparantie maakt het onmogelijk exact te beoordelen welke impact de personalisering van Facebook heeft op de mensenrechten wanneer de overheid Facebook-pagina's gebruikt.

Toegang door buitenlandse overheden buiten de EU kan ook tot risico's leiden voor de mensenrechten van de personen die een Facebook-pagina van de Nederlandse overheid bezoeken. Overheidsinstanties kunnen op allerlei manieren toegang tot de persoonsgegevens verkrijgen, door gebruik te maken van de informatie die op openbare Facebook-pagina's staat of door onderzoek te doen naar de informatie die advertentiebedrijven verzamelen over bezoekers. Ze kunnen Facebook ook dwingen (of Facebook-medewerkers hacken/chanteren/omkopen) om profielgegevens te verstrekken die Facebook over bezoeken aan een overheidspagina heeft afgeleid. Dit kan leiden tot intimidatie of (cyber)aanvallen tegen individuele bezoekers van een overheidspagina of tot mensenrechtenschendingen wanneer deze mensen naar derde landen reizen. Zoals beschreven in de DPIA, volgt uit de rechtspraak van het Europese Hof van Justitie over doorgifte van persoonsgegevens naar Amerika dat er een reëel risico bestaat dat opsporings- en inlichtingendiensten in de VS toegang krijgen tot door Facebook verzamelde persoonsgegevens. Daarom heeft de Ierse toezichthouder op de gegevensbescherming een ontwerp-verbod uitgevaardigd op de toekomstige doorgifte van gegevens van Facebook-klanten uit de EU naar de VS.

Het rapport beoordeelt dat overheidsorganisaties moeten stoppen met het gebruik van Facebook-pagina's als communicatiemiddel, vanwege de grote risico's voor de mensenrechten van de pagina-bezoekers. Dit advies kan veranderen als Facebook zich als zeer groot online platform moet houden aan nieuwe Europese regels over digitale diensten uit de Digital Services Act, die meer verantwoording en transparantie over de risico's van algoritmische dienstverlening voor mensenrechten verplicht voor zeer grote online platforms. Nog dit jaar zullen zeer grote online platforms zo een risico-inschatting en een overzicht van mitigerende maatregelen moeten aanleveren aan de Europese Commissie, die de naleving van die regels door Facebook als toezichthouder zal beoordelen.