AUTORITEIT
PERSOONSGEGEVENS

Datum
30 november 2022

Onderwerp
Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik

Geachte (plv.) leden van de Kamercommissies voor Justitie en Veiligheid en Digitale Zaken,

Op 11 mei heeft de Europese Commissie het voorstel voor de Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik gepresenteerd. Met deze brief vraagt de Autoriteit Persoonsgegevens (AP) aandacht voor een drietal punten van zorg bij dit voorstel.

Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik
De AP vindt vanzelfsprekend dat kindermisbruik hard moet worden aangepakt, maar het huidige voorstel vormt een te groot risico voor de rechten en vrijheden van burgers. In het bijzonder is de inbreuk op het recht op privacy en bescherming van persoonsgegevens te groot. Ook de European Data Protection Board (EDPB), het samenwerkingsverband van de Europese privacytoezichthouders, en de Europese toezichthouder voor gegevensbescherming (EDPS) hebben hun zorgen geuit.[1]

Het voorstel zal chatapps, sociale media, maar ook internetproviders verplichten om de communicatie van hun gebruikers te scannen op beelden van kindermisbruik. Bovendien zal worden gescand op pogingen om kinderen online te benaderen met het doel ze te misbruiken, ook wel '*grooming*'. Het nu voorliggende voorstel verplicht communicatiediensten niet alleen om berichten te bekijken, maar zelfs om gesproken communicatie af te luisteren.

Punten van zorg AP:

1. Er ontstaat een te groot risico dat communicatiediensten bij *alle* communicatie van *alle* burgers in de Europese Economische Ruimte (EER) mee zullen kijken én luisteren;
2. Er is een groot risico op ondermijning van het gebruik van versleutelde communicatie (zogeheten *end-to-end* encryptie);
3. De AI-software die waarschijnlijk wordt ingezet maakt fouten en kan vooroordelen bevatten, waardoor burgers ten onrechte als potentieel 'verdacht' worden aangemerkt.

[1] EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse | European Data Protection Board (europa.eu)

Datum
30 november 2022

Toelichting punten van zorg

In de voorliggende brief deelt de AP haar grootste zorgen over het voorstel van de Europese Commissie.

1. Risico op het meekijken en afluisteren van *alle* communicatie van *alle* burgers in de EER

Het Commissievoorstel kan ertoe leiden dat het afluisteren van praktisch alle vormen van communicatie van alle gebruikers in de EER wordt toegestaan. Dit maakt iedereen bij voorbaat tot potentieel 'verdachte' en is een onacceptabele inbreuk op het recht op briefgeheim. Het briefgeheim is een essentieel onderdeel van het recht op privacy en de bescherming van persoonsgegevens.[2] Elke inbreuk op deze rechten moet noodzakelijk en proportioneel zijn voor het nagestreefde doel. Het huidige voorstel voldoet niet aan deze eisen, met alle gevaren van dien.

Het voorstel is niet concreet genoeg over de voorwaarden waaronder communicatiediensten moeten onderzoeken of er sprake is van beelden van kindermisbruik of pogingen om kinderen online te benaderen met het doel ze te misbruiken (*'grooming'*). Eén van de voorwaarden stelt bijvoorbeeld dat er sprake moet zijn van een 'significant risico' op misbruik van de dienst. Er worden echter onvoldoende duidelijke en inhoudelijke criteria gegeven om te bepalen wanneer er sprake is van zo'n 'significant risico'. Ook kunnen communicatiediensten worden verplicht om voor langere periodes – tussen de 12 en 24 maanden – mee te kijken en luisteren met alle communicatie van gebruikers. Met andere woorden: partijen kunnen verplicht worden om zonder goede reden mee te kijken en luisteren met alle communicatie tussen gebruikers. Ook kan dit leiden tot willekeur over wie er wordt afgeluisterd. Dit creëert rechtsonzekerheid.
Praktisch gezegd: iedere Nederlander kan op ieder willekeurig moment worden afgeluisterd. De AP benadrukt daarom de noodzaak voor het aanbrengen van duidelijkere criteria voor het bepalen wanneer iemand mag worden afgeluisterd.

De maatregelen voor het opsporen van *grooming* vormen in het bijzonder een zeer grote inbreuk op het recht op privacy. Niet alleen foto's, maar ook geschreven en gesproken communicatie zal worden bekeken en afgeluisterd. Bovendien kan communicatie in de vorm van geluidsmateriaal niet alleen achteraf, maar ook *live* kan worden afgeluisterd. De AP vindt dit een te vergaande inbreuk en vindt dat deze betreffende artikelen uit het voorstel moeten worden verwijderd.

2. Versleuteling is essentieel

Veel communicatie wordt online beveiligd door middel van versleuteling. *End-to-end* encryptie is hiervoor de meest gebruikte vorm. Door het versleutelen van gegevens kunnen alleen de verzender en de ontvanger de berichten lezen. Versleuteling is dus een zeer belangrijke maatregel voor de bescherming van het privéleven en het briefgeheim.

Het onderscheppen en analyseren van persoonlijke communicatie staat haaks op het doel van *end-to-end* encryptie: communicatie vertrouwelijk houden tussen ontvanger en verzender. Er lijkt op het moment ook

[2] Zoals neergelegd in art. 7 en 8 van het Europees Handvest.

nog geen technologische oplossing voor het opsporen van beeldmateriaal in versleutelde vorm. Dit betekent dat communicatiediensten mogelijk hun versleuteling zullen ondermijnen om aan hun verplichtingen onder het voorstel te kunnen voldoen. Bijvoorbeeld door toch een achterdeur in te bouwen die de communicatiediensten kunnen gebruiken, of misschien zelfs te kiezen voor een algehele stop op het gebruik van versleuteling. Zelfs de Europese Commissie erkent dat het scannen van communicatie voor beelden van kindermisbruik wordt beperkt bij gebruik van *end-to-end* encryptie. De potentiele ondermijning van versleuteling heeft impact op de privacy van alle gebruikers, omdat dan álle communicatie minder goed wordt beveiligd. De AP raadt daarom aan om expliciet in het voorstel op te nemen dat het voorstel niet als doel heeft *end-to-end* encryptie te verbieden of te verzwakken.

De AP wijst erop dat op 30 juni 2022 een motie is ingediend door de Tweede Kamerleden Van Raan, Van Baarle, Van Ginneken, Leijten en Van Weerdenburg voor het behoud van *end-to-end* encryptie en het briefgeheim.[3] De minister van Justitie en Veiligheid heeft op 23 september 2022 in een brief aangegeven hieraan gevolg te geven en voorstellen die *end-to-end* encryptie onmogelijk maken niet te steunen.[4] Dit is in lijn met de visie van de AP.

3. Software maakt fouten en bevat potentieel vooroordelen

Het voorstel richt zich op drie vormen van kindermisbruik: beeldmateriaal van kindermisbruik al bekend bij opsporingsdiensten, nog onbekend beeldmateriaal en *grooming*. Materiaal op platforms kan worden vergeleken met een database van bekend beeldmateriaal van kinderenmisbruik. Hiervoor gebruikt men 'matching'-technologie met een relatief lage foutmarge. Voor het opsporen van nog onbekend beeldmateriaal en *grooming* kunnen deze 'matching'-technologieën niet worden ingezet en zal waarschijnlijk algoritmische software worden gebruikt. Er is echter nog zeer weinig bekend over het op grote schaal inzetten van deze technologieën en de risico's daarvan. Wel zijn er indicaties dat deze technologieën meer fouten maken en bestaat bij de inzet van algoritmes het risico op vooroordelen en discriminatie.

Zo blijkt uit de *Impact Assessment* van de Europese Commissie dat bepaalde technologieën die ingezet kunnen worden voor het opsporen van *grooming* voor ongeveer 88% van de gevallen accuraat zijn. Dat betekent dat er in 12% van de gevallen een vals-positieve uitkomst kan zijn. Over welke technologieën mogelijk ingezet kunnen worden voor het afluisteren van gesproken communicatie bevat dit stuk geen informatie. Gezien het feit dat alle EU-gebruikers potentieel afgeluisterd worden, betekent zelfs een zeer laag percentage onterechte aanwijzingen voor misbruik of *grooming* dat er nog steeds erg veel onschuldige gebruikers geraakt worden. Bovendien kunnen de gevolgen voor betrokkenen die ten onrechte door een AI-systeem worden beschuldigd van seksueel kindermisbruik en *grooming* zeer ingrijpend zijn.

[3] Motie van het lid Van Raan c.s. over end-to-endencryptie in stand houden
[4] Uitvoering van de motie van het lid Van Raan c.s. over end-to-endencryptie in stand houden (Kamerstuk 26643-885)

Datum
30 november 2022

Er is meer informatie nodig over de effectiviteit en de risico's van deze technologieën en de criteria waaraan de software moet voldoen. Zonder deze informatie en waarborgen is er beperkt zicht op de hoeveelheid burgers die ten onrechte door een AI-systeem beschuldigd kunnen worden van *grooming* en kindermisbruik.

Conclusie

De AP hoopt dat deze punten van aandacht worden meegenomen bij uw voorbereiding voor het schriftelijk overleg van de vaste commissie voor Digitale zaken over 'de uitvoering van de motie van het lid Van Raan over *end-to-end*encryptie in stand houden' van 2 december en/of het commissiedebat van de vaste commissie voor Justitie en Veiligheid over de JBZ-Raad van 8 en 9 december. Mocht u naar aanleiding van deze brief nog vragen hebben, schroom dan niet om contact op te nemen.

Hartelijke groet,

Aleid Wolfsen

Voorzitter Autoriteit Persoonsgegevens