Bert Hubert
bert@hubertnet.nl
https://berthub.eu/

Pijnacker-Nootdorp, 17 september 2024

Geachte ministers,

Ondanks dat er al veel gezegd[1] en geschreven[2] is over de CSAM-verordening wil ik hier graag toch nog enige woorden toevoegen. Ten eerste over rechtstatelijkheid, ten tweede over de enorme impact op gezinnen van de toepassing van feilbare detectietechnologie, en ten derde over of het een goed idee is om "big tech" nu in vertrouwen te nemen om onze bevolking in de gaten te houden. Afsluitend wijd ik wat woorden aan wat we beter eerst zouden kunnen doen om kinderen te beschermen.

Om te beginnen, met deze verordening zullen voor het eerst onze meest private berichten in opdracht van de overheid door big tech gemonitord worden op potentieel strafbare inhoud. Indien deze wordt gevonden in bijvoorbeeld ons WhatsApp-verkeer gaat er een melding naar Europol en de lokale politie. Voor de duidelijkheid, dit gaat ook over de appgroep van uw afdeling of kabinet, al kunnen *sommige* ministeries een uitzondering krijgen[3].

Ik kan niet genoeg benadrukken wat voor een drempel we hiermee over zouden gaan. Buiten dictaturen is dit soort bulk monitoring van privé-berichten nog nooit vertoond[4]. Ervaring leert dat als een dergelijke hobbel eenmaal genomen is dit soort *surveillance* ook acceptabel wordt voor andere doelen. Europol noemde als voorbeeld dat dit ook zou werken tegen witwassen.

Weet welke deur we hiermee op een kier zetten.

Ten tweede, de gevolgen van een melding bij Europol en de lokale politie kunnen groot zijn. In Europa is bulk *secret surveillance* door inlichtingendiensten schoorvoetend door de hoogste rechters geaccepteerd[5], maar alleen omdat deze omgeven wordt door een streng toezichtregime wat adequaat en effectief moet voorkomen dat dit soort bulk afluisteren leidt tot onbedoelde gevolgen. Iemand die in *bulk* door een inlichtingen- of veiligheidsdienst is afgeluisterd heeft daar kort gezegd praktisch geen last van – het is staatsgeheim en komt niet in het strafrecht terecht.

Dit is geheel anders bij een melding van vermoedelijk kinderpornografisch materiaal. De CSAM-verordening bevat geen procedure hoe lokale politiemachten om moeten gaan met een melding. Terloops, de melding wordt op basis van GPS-coördinaten doorgesluisd naar het meest geschikte politiebureau. Dit kan zomaar op uw vakantieadres zijn waar u de taal slecht spreekt.

---

[1] Video rondetafelgesprek Client Side Scanning (CSS)

[2] Bijdrage Bert Hubert rondetafelgesprek Tweede Kamer Client Side Scanning

[3] Nationale veiligheidsdiensten, politie, openbare veiligheidsdiensten en militairen hebben in artikel 7(8)(d) van de verordening een vrijstelling van monitoring gekregen. "Detection does not apply to accounts used by the State for national security purposes, maintaining law and order or military purposes."

[4] De verordening maakt juridische manoeuvres dat de detectie technisch gezien vrijwillig plaatsvindt en op de telefoon van de gebruiker. De vrijwilligheid bestaat eruit dat de gebruiker anders geen berichten kan versturen, en specifiek *waar* de detectie plaatsvindt is irrelevant.

[5] Recente uitspraken van het EHRM en de totstandkoming van Conventie 108+ in relatie tot het stelsel van toezicht op inlichtingen- en veiligheidsdiensten (BZK interne analyse)

Zo'n melding zal minimaal leiden tot opname in databases. We weten inmiddels uit ruime ervaring dat ook geheel onschuldige burgers jaren lang last kunnen hebben van het voorkomen in zo'n database. Zeker als de politie (zoals wordt voorspeld) geen tijd heeft om iedere melding tijdig te onderzoeken en eventueel af te voeren. In het voorstel staat overigens opgenomen dat de EU ook onterecht bevonden meldingen blijvend opslaat voor onderzoek (!).

De voorgestelde detectie-technologieën zijn allen 'fuzzy[6]', in de zin dat deze ook aanslaan op foto's die niet exact overeenkomen met bekend materiaal. Ook is het voor aanbieders van interpersoonlijke communicatiediensten toegestaan om AI in te zetten voor detectie, en worden ze hiertoe zelfs aangemoedigd in de verordening.

Een nadeel van dit soort technieken, zelfs als ze alleen kijken naar "bekend materiaal", is dat het eenvoudig is om een "foute" foto om te bouwen zodat er geen match meer is, en, omgekeerd een onschuldige foto zo aan te passen dat hij gematched gaat worden als verdacht[7]. Het is nogal wat om onze fundamentele rechten op te geven voor technologie die zo weinig effectief is en die ook zo makkelijk gemanipuleerd kan worden.

Dit soort detectiealgoritmes is eerder ingezet bij *publieke* websites waar foto's gedeeld kunnen worden. Materiaal herkend als verdacht wordt dan verwijderd en mogelijk verliest de uploader toegang tot zijn account.

Dit zijn relatief kleine gevolgen, en mogelijk is de technologie daar nu goed genoeg voor.

Maar waar we nu op afstevenen is dat dergelijke algoritmes ons effectief aangeven bij een politiemacht, die vervolgens weinig beperkt is in wat er gebeurt. Dit kan geheel verkeerd aflopen.

Dat de CSAM-verordening in juridische taal stelt dat de gebruikte technologie er nooit naast mag zitten betekent overigens nog niet dat dit vervolgens ook zo is.

Ten derde, Europa heeft op allerhande vlakken het aan de stok met "big tech". Bedrijven als Google, Facebook/Meta en Apple onttrekken zich stelselmatig aan onze wetgeving. Slechts na jarenlang procederen luisteren deze "multinationale platformbedrijven" (MPB's) naar onze gerechtelijke uitspraken. Tegelijkertijd zijn we in Europa nu zeer afhankelijk van big tech, zoals ook uiteengezet in het recente boek van Marietje Schaake, "De tech coup. Hoe tech is gaan regeren en we de macht weer terugwinnen"[8].

De CSAM-verordening leunt voor zijn succes vrijwel geheel op de actieve inzet van big tech bedrijven. Als deze bedrijven matige technologie gebruiken zijn de gevolgen niet te overzien. Als de juiste "checks and balances" niet ingericht worden kunnen geheel de verkeerde mensen gemeld worden bij Europol. Als de beveiliging van de technologie niet op orde is lekt mogelijk uit precies wie er al bij de politie gemeld is.

Is dit nu het moment om juist "big tech" te voorzien van een faciliteit waarmee levens geruïneerd kunnen worden? Zeker als we weten hoe slecht deze bedrijven zich onderwerpen aan onze wetgeving? Terloops dient ook de EU de nodige hoeveelheid software te (laten) ontwikkelen om de stroom meldingen veilig af te handelen, maar bijvoorbeeld Europol heeft het zelf moeite met informatiebeveiliging[9]. En terloops, wat betekent het voor onze agenda digitale open strategische autonomie[10]?

Naast deze drie punten wil ik het volgende in overweging geven. De voorliggende plannen gaan honderden miljoenen euro's kosten. Direct of indirect gaan we hier allemaal de rekening voor betalen. Tegelijkertijd klagen

[6] Detectie van al bekend materiaal moet ook om kunnen gaan met kopieën of vervormde varianten van bestaande foto's. Zo kunnen ook onschuldige foto's of delen van foto's leiden tot een match. Echt alleen letterlijke 100% matches detecteren mist te veel om nog nuttig te zijn.

[7] Blogpost van Universitair Hoofddocent Jaap-Henk Hoepman, End-to-end encryptie en de risico's van client-side scanning

[8] Bespreking in NRC

[9] Minister Yesilgöz: datalek schaadt vertrouwen in Europol en brengt personeel in gevaar.

[10] Agenda Digitale Open Strategische Autonomie

zedenrechercheurs over tekort aan mensen en middelen[11]. Als we daadwerkelijk kinderen willen beschermen, zouden we daar dan niet eerst de tekorten op moeten lossen? Dit voor we technologie uitrollen die alleen maar tot meer werk gaat leiden daar?

Samenvattend, met de CSAM-verordening zetten we een staatsrechtelijke deur op een kier om onze meest privé-communicatie stelselmatig te laten monitoren door overheden. De gevolgen van meldingen uit die monitoring kunnen enorm zijn, en de voorgestelde technologie is nog nooit ingezet voor zulke belangrijke beslissingen. De kwaliteit en het succes van dit alles staat of valt bij het enthousiasme en de inzet van “big tech”, een groep bedrijven die zich keer op keer onttrekt aan onze wet- en regelgeving. En juist zij komen nu in een positie waarin ze levens kunnen ruineren.

Ik hoop dat het bovenstaande u beweegt in aankomende overleggen de CSAM-verordening niet te steunen.

Met vriendelijke groet,

Bert Hubert

[11] Technische Briefing “Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik”, Tweede Kamer, 4 oktober 2022, op minuut 52