Aan:

- Minister van Justitie en Veiligheid
- Staatssecretaris Rechtsbescherming
- Minister van Binnenlandse Zaken en Koninkrijksrelaties
- Staatssecretaris Digitalisering en Koninkrijksrelaties
- Minister van Economische Zaken
- Minister van Buitenlandse Zaken

Afschrift aan de vaste commissie van Justitie en Veiligheid, Economische Zaken en Digitale Zaken van de Tweede Kamer.

18 september 2024, Amsterdam, Breukelen en Noordwijk

Geachte bewindspersoon,

Op 16 september jongstleden stuurde de minister van Justitie en Veiligheid een brief aan de Tweede Kamer over de onderhandelingen over de EU-Verordening ter bestrijding van online seksueel kindermisbruik (CSAM-Verordening).[1] In deze brief geeft de minister aan dat het kabinet nog overlegd over haar standpunt inzake het recente wijzigingsvoorstel van de Hongaarse voorzitter van de Raad.[2] De minister geeft tevens aan dat oog nodig is voor andere belangen dan enkel dat van de opsporing van strafbare feiten. In het verlengde daarvan doen we graag een dringend verzoek aan u.

Belang van vertrouwelijkheid in een digitale maatschappij

Het belang van de vertrouwelijkheid van communicatie is onbetwist. Niet alleen is het een fundamenteel beginsel om als maatschappij te functioneren; het is ook van essentieel belang voor communicatie van burgers, het bedrijfsleven en de overheid. Het is niet voor niets een van de fundamentele grondrechten. In onze snel ontwikkelende digitale maatschappij is encryptie hét middel om die vertrouwelijkheid van communicatie te beschermen. Sterker nog, encryptie is zelfs een van de weinige middelen, zo niet de enige, die we, als burgers, bedrijfsleven en overheid, daartoe hebben. Wanneer encryptie ondermijnd wordt, wordt de vertrouwelijkheid van al het economische en maatschappelijke verkeer ondermijnd.

Kabinetsstandpunt encryptie: zorgvuldige afweging

Het belang van encryptie wordt ook door uw kabinet onderschreven. Al acht jaar hanteert u het standpunt dat “het niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie”.[3] U kwam destijds tot deze conclusie na een zorgvuldige afweging van drie relevante belangen.

---

[1] Kamerbrief over kabinetsstandpunt CSAM verordening, 16 september 2024
[2] Het wijzigingsvoorstel van de Hongaarse voorzitter heeft als kenmerk 12406/24 (9 september 2024) en is gebaseerd op het eerdere wijzigingsvoorstel met als kenmerk 11277/24. Dit zijn voorstellen om te komen tot een zogenaamde algemene oriëntatie binnen de Raad.
[3] Kabinetsstandpunt over encryptie, 4 januari 2016

In uw brief aan het parlement noemt u allereerst het belang om de veiligheid in Nederland te waarborgen, door het opsporen en vervolgen van strafbare feiten. U overwoog ten tweede het belang van burgers, bedrijven en de overheid bij maximale veiligheid van onze digitale infrastructuur. Tot slot onderschreef u het grondrecht op eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim van burgers. U heeft destijds veel lof ontvangen voor deze zorgvuldige afweging en heldere conclusie. Ook het Nederlandse parlement kan zich vinden in de conclusie, zoals duidelijk wordt uit de zeer breed ondersteunde motie van Van Raan.[4]

Client side scanning ondermijnt vertrouwelijkheid van communicatie

Instemmen met het voorstel betekent instemmen met de (ongerichte) inzet van *client side scanning*. In het voorstel van de Europese Commissie wordt een zogenaamd detectiebevel geïntroduceerd.[5] Op grond daarvan zouden autoriteiten een communicatiedienst zoals Signal en WhatsApp kunnen dwingen tot het monitoren van alle berichtjes van hun gebruikers.

Het voorliggende voorstel zegt te beogen encryptie niet te verzwakken.[6] Om toch de inhoud van de berichten te kunnen monitoren, ook als de vertrouwelijkheid van communicatie wordt beschermd door het gebruik van encryptie, is het gebruik van *client side scanning* bedacht. Daarmee zouden berichten beoordeeld moeten worden vóór de daadwerkelijke verzending, en daarmee voordat de encryptie daadwerkelijk wordt toegepast. Hoe je het ook wendt of keert, met de inzet van *client side scanning* wordt het doorbreken van de vertrouwelijkheid van communicatie doelbewust bewerkstelligd. Het doet daarmee afbreuk aan de bescherming die nu juist beoogd wordt met het toepassen van encryptie. Het gebruik van *client side scanning* kan dan ook gezien worden als het omzeilen van encryptie.

Ontbrekende zorgvuldige afweging van alle relevante belangen

Het doorbreken van die vertrouwelijkheid van communicatie en het omzeilen van encryptie is een enorme en onomkeerbare stap. Als we dat, als maatschappij, al zouden willen, dan alleen na een zorgvuldige afweging van alle grondrechten en belangen. Tot op heden hebben we het kabinet deze zorgvuldige afweging nog niet zien maken. Vooralsnog lijkt alleen het belang van de opsporing en vervolging van strafbare feiten het enige dat in uw afwegingen is meegenomen.

We roepen het kabinet dan ook op om in de afweging van haar standpunt inzake de voorgestelde Verordening eerst een zorgvuldige afweging van alle relevante grondrechten en belangen te maken rond de inzet van *client side scanning*. Die belangen zouden dan in ieder geval de belangen moeten zijn die ook zijn overwogen bij de totstandkoming van het kabinetsstandpunt over encryptie, dus, kort gezegd, opsporing, grondrechten, economie en online veiligheid. Dit complexe vraagstuk vereist een zorgvuldige, democratisch geborgde, overweging vanwege de verstrekkende gevolgen voor de fundamentele rechten van

---

[4] Motie van het lid Van Raan c.s. over end-to-endencryptie in stand houden, 30 juni 2022
[5] Artikel 7 van de voorgestelde Verordening
[6] Zie recital 26 en 26a en artikel 1(5) van het Hongaarse wijzigingsvoorstel

mensen. We verzoeken u deze belangenafweging voor te leggen aan het parlement voordat u enig onomkeerbaar besluit neemt.

Voorschot op de te maken afweging en conclusie

De ondergetekende organisaties kunnen het zich niet voorstellen dat de zorgvuldige afweging van de eerder genoemde grondrechten en belangen in de context van *client side scanning* tot een wezenlijk andere conclusie kan leiden dan die in het kabinetsstandpunt over encryptie. Immers, het kabinet onderschrijft het belang van encryptie voor de veiligheid op internet, ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven, en voor de Nederlandse economie. Omdat *client side scanning* de bescherming die encryptie beoogt te bewerkstelligen fundamenteel ondermijnt, ligt het voor de hand dat de conclusie moet zijn dat 1) het onwenselijk is om wettelijke beperkingen te nemen ten aanzien van de ontwikkeling, beschikbaarheid en toepassing van encryptie én 2) het onwenselijk is in plaats daarvan de inzet van *client side scanning* af te dwingen.

Vanzelfsprekend zijn we graag bereid tot een nadere toelichting, mocht daartoe behoefte bestaan.

Met vriendelijke groet,

- Amnesty International Nederland
- Bits of Freedom
- Cyberveilig Nederland
- NLdigital

Contact
- [redacted]
- [redacted]