Betoog
Belle van der Velde
500906306
25/09/2026

De overheid moet geen toegang krijgen tot end-to-end-encryptie, ook niet bij een vermoeden van ernstige criminaliteit

Tegenwoordig gebruiken veel mensen apps zoals WhatsApp, Telegram en Signal om met elkaar contact te houden. Deze apps gebruiken vaak end-to-end-encryptie. Dit betekent dat alleen de verzender en ontvanger de berichten kunnen lezen. Hierdoor blijven gesprekken privé en zijn gegevens beter beschermd tegen hackers. Toch wil de overheid in sommige gevallen toegang kunnen krijgen tot deze berichten, bijvoorbeeld bij een vermoeden van criminaliteit. Zo werkte de overheid in 2021 aan een plan om de beveiliging van chatberichten te verzwakken, zodat berichten van verdachten onderschept konden worden (NOS, 2021a). Ik ben het hier niet mee eens. Ik vind dat de overheid geen toegang moet krijgen tot end-to-end-encryptie, omdat dit ook gevolgen kan hebben voor de veiligheid en privacy van andere mensen.

Ten eerste is end-to-end-encryptie belangrijk voor journalisten en hun bronnen. Journalisten praten soms met mensen die gevoelige informatie geven over bijvoorbeeld bedrijven of de overheid. Deze mensen moeten erop kunnen vertrouwen dat hun gesprekken geheim blijven. Als de overheid toegang kan krijgen tot versleutelde berichten kunnen bronnen zich misschien minder veilig voelen om informatie te delen. De Vereniging voor Onderzoeksjournalisten noemde het verzwakken van encryptie daarom een groot risico voor de bronbescherming en tekende een verklaring tegen het plan van de overheid om encryptie te verzwakken (NOS, 2021b). Encryptie is dus niet alleen handig voor gewone gesprekken, maar kan ook belangrijk zijn voor mensen die gevoelige informatie naar buiten willen brengen.

Daarnaast kan het verzwakken van encryptie voor problemen met digitale veiligheid zorgen. Om versleutelde berichten te kunnen lezen, is namelijk een extra digitale sleutel nodig. Die sleutel kan gestolen en misbruikt worden. Volgens Bits of Freedom gaan criminelen zo'n achterdeur uiteindelijk zelf gebruiken (NOS, 2021a). Sterke encryptie beschermt daarom niet alleen criminelen, maar ook gewone burgers tegen hackers, fraude en het stelen van persoonlijke gegevens. Bovendien is zo'n achterdeur niet eens nodig. De politie kan versleutelde berichten ook op een andere manier lezen. Bij ernstige misdrijven mag zij namelijk de telefoon van een verdachte binnendringen (Verhaert, 2023). Zo las de politie vijf maanden mee met criminelen die de chatdienst Exclu gebruikten (NOS, 2023). Het lijkt mij daarom niet verstandig om de beveiliging voor iedereen zwakker te maken om een groep criminelen makkelijker op te kunnen sporen.

Een ander probleem is dat mensen misschien minder vertrouwen krijgen in digitale communicatie. Als mensen weten dat de overheid mogelijk toegang kan krijgen tot hun berichten kunnen ze voorzichtiger worden met wat ze online bespreken. Marleen Stikker noemt dit ook in haar boek Het internet is stuk. Volgens haar gaan mensen zich anders gedragen als ze weten dat iemand misschien meekijkt. Ze geeft als voorbeeld de Sleepwet uit 2017, waardoor de overheid ook gegevens mag verzamelen van mensen die zelf niet verdacht zijn. Zo worden burgers behandeld alsof ze verdacht zijn tot het tegendeel bewezen is. Dit kan bijvoorbeeld gevolgen hebben voor mensen die persoonlijke of gevoelige informatie willen delen. Denk aan iemand die advies vraagt aan een advocaat of arts of iemand die een probleem op het werk wil bespreken. Ook bedrijven versturen belangrijke informatie via digitale communicatie. Dit laat

zien dat toegang tot versleutelde berichten niet alleen gevolgen heeft voor criminelen, maar ook voor mensen die niets verkeerd doen.

Toch is er ook een belangrijk argument vóór toegang. Criminelen gebruiken namelijk ook versleutelde communicatie. Bij onderzoeken naar EncroChat en Sky ECC zijn berichten gevonden die te maken hadden met internationale drugshandel. Zo begon een onderzoek met onderschepte chats tussen verdachten uit Leeuwarden, die handelden in cocaïne, cannabis en crystal meth in Nederland en Duitsland (Openbaar Ministerie, 2021).Dit laat zien dat digitale communicatie de politie kan helpen bij het onderzoeken van ernstige criminaliteit.

Ook heeft de overheid de verantwoordelijkheid om burgers te beschermen tegen ernstige criminaliteit. Bij een sterk vermoeden van criminaliteit kan digitale communicatie belangrijk bewijs bevatten. Europese politiechefs waarschuwden in 2024 dat end-to-end-encryptie het verzamelen van bewijs bij zware misdaad zoals terrorisme, kindermisbruik en drugssmokkel tegenhoudt (Politie, 2024). De politie moet dus wel mogelijkheden hebben om ernstige misdaad te onderzoeken, anders kunnen criminelen digitale technologie gebruiken om zich makkelijker voor de politie te verbergen.

Toch vind ik deze argumenten niet sterk genoeg om end-to-end-encryptie voor iedereen zwakker te maken. Hier botsen namelijk twee publieke waarden, veiligheid en privacy. De overheid wil burgers beschermen tegen criminaliteit, maar burgers hebben ook recht op privé communicatie. Het probleem is dat een verandering niet alleen gevolgen heeft voor criminelen. Ook anderen kunnen hierdoor minder veilig communiceren. Dit kan ten koste gaan van de publieke waarden. We moeten dus niet alleen kijken naar wat de overheid technisch kan doen, maar ook naar de gevolgen daarvan voor de samenleving.

Daarom vind ik dat de overheid geen toegang moet krijgen tot end-to-end-encryptie. Natuurlijk moet de politie ernstige criminaliteit kunnen onderzoeken. Toch moet dit niet ten koste gaan van de digitale veiligheid van alle burgers. Een betere oplossing is daarom een middenweg. Hierbij zou de politie onder strenge regels gericht onderzoek kunnen doen naar specifieke verdachten of criminele chatdiensten, zoals bij EncroChat en Exclu. Er moet dan goed worden gekeken wanneer dit echt nodig is en wie hiervoor toestemming moet geven.

Kortom, criminelen kunnen end-to-end-encryptie misbruiken, maar dat betekent niet dat de beveiliging voor alle burgers moet worden verzwakt. Sterke encryptie beschermt journalisten en hun bronnen, gewone burgers en bedrijven. Een betere middenweg is dat de politie gericht onderzoek doet naar verdachten, in plaats van de encryptie voor iedereen te verzwakken. Criminaliteit moet kunnen worden opgespoord, maar zonder dat de digitale veiligheid van miljoenen andere mensen in gevaar komt.

Bronnen:

Goslings, Z. (2023, 29 oktober). *End-to-end encryptie: heet hangijzer voor opsporingsdiensten, zevende hemel voor criminelen*. Rechtencircuit. https://www.rechtencircuit.nl/end-to-end-encryptie-heet-hangijzer-voor-opsporingsdiensten-zevende-hemel-voor-criminelen/

Kabinet trekt harde grens bij Europese chatcontrole. (2026, 22 september). iBestuur. https://ibestuur.nl/digitale-toekomst-eu/eu-wetgeving/kabinet-trekt-harde-grens-bij-europese-chatcontrole

NOS Nieuws. (2021 a, 4 maart). *Overheid werkt aan plan voor afzwakken encryptie: "Taak voor nieuw kabinet"*. NOS. https://nos.nl/artikel/2371134-overheid-werkt-aan-plan-voor-afzwakken-encryptie-taak-voor-nieuw-kabinet

NOS Nieuws. (2021b, [datum checken]). *Brede coalitie richt zich tegen regeringsplannen om encryptie te verzwakken*. NOS. https://nos.nl/artikel/2372017-brede-coalitie-richt-zich-tegen-regeringsplannen-om-encryptie-te-verzwakken

NOS Nieuws. (2023, 3 februari). *Politie leest vijf maanden mee met versleutelde berichten, 42 arrestaties*. NOS. http://nos.nl/artikel/2462344-politie-leest-vijf-maanden-mee-met-versleutelde-berichten-42-arrestaties

Openbaar ministerie. (2021, 18 november). *Encro- en SKY ECC-chats leiden naar verdachten internationale drugshandel*. https://www.om.nl/actueel/nieuws/2021/11/18/encro--en-sky-ecc-chats-leiden-naar-verdachten-internationale-drugshandel

Politie. (2024, 2 mei). *Politie luidt noodklok over encryptie op digitale platforms*. https://www.politie.nl/nieuws/2024/mei/2/00-politie-luidt-noodklok-over-encryptie-op-digitale-platforms.html

Verhaert, J. (2023, 20 juni). *De hackbevoegdheid in de praktijk*. Bijzonder Strafrecht. https://www.bijzonderstrafrecht.nl/home/artikel-de-hackbevoegdheid-in-de-praktijk