Betoog
Belle van der Velde
500906306
25/09/2026

De overheid moet toegang kunnen krijgen tot end-to-end-encryptie 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. 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. Hierdoor kunnen belangrijke punten minder snel naar buiten komen. Volgens de NOS is veilige communicatie daarom belangrijk voor journalisten en activisten. 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. Als de overheid makkelijker binnen kunnen komen, kunnen hackers daar bijvoorbeeld ook gebruik van maken. Een systeem dat bedoeld is om de politie te helpen, kan dan juist een zwakke plek worden. Als hackers zo'n zwakke plek vinden, kunnen zij misschien toegang krijgen tot gegevens die eigenlijk goed beveiligd zouden moeten zijn. Sterke encryptie beschermt daarom niet alleen criminelen, maar ook gewone burgers tegen hackers, fraude en het stelen van persoonlijke gegevens. 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. 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. Als mensen het gevoel krijgen dat hun gesprekken niet meer echt privé zijn, kan dat ervoor zorgen dat ze digitale communicatie minder vertrouwen. 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. Via deze berichten kunnen ze bijvoorbeeld afspraken maken over drugshandel, geld en vervoer. Bij onderzoeken naar EncroChat en Sky ECC zijn berichten gevonden die te maken hadden met internationale drugshandel. Dit laat zien dat digitale communicatie de politie soms kan helpen bij het onderzoeken van ernstige criminaliteit. Zonder deze informatie kan het moeilijker zijn om te ontdekken wat verdachten met elkaar bespreken en welke rol zij hebben binnen een criminele organisatie.

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. Het is daarom begrijpelijk dat de politie toegang wil tot zulke informatie. Elektronisch bewijs wordt steeds belangrijker bij strafrechtelijke onderzoeken. 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. Het probleem is namelijk dat een verandering niet alleen gevolgen heeft voor criminelen. Ook anderen kunnen hierdoor minder veilig communiceren. Dit kan ten koste gaan van privacy, veiligheid en vrijheid. 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 directe toegang moet krijgen tot end-to-end-encryptie. Natuurlijk moet de politie ernstige criminaliteit kunnen onderzoeken en moet er gezocht worden naar bewijs. Toch moet dit niet ten koste gaan van de digitale veiligheid van alle burgers. Er zou daarom eventueel gezocht kunnen worden naar een middenweg. Hierbij zou bijvoorbeeld onder strenge regels toegang kunnen worden gegeven tot bepaalde versleutelde berichten. Er moet dan goed worden gekeken wanneer dit echt nodig is en wie hiervoor toestemming moet geven. Op die manier kan de politie misschien worden geholpen, zonder dat de privacy en veiligheid van alle burgers minder worden.

Kortom, criminelen kunnen end-to-end-encryptie misbruiken, maar dat betekent niet dat de beveiliging voor alle burgers moet worden verzwakt. Sterke encryptie zorgt voor meer vrijheid en veiligheid. We moeten daarom niet alleen kijken naar de veiligheid van de overheid, maar ook naar de privacy en veiligheid van burgers. Een goede middenweg zou daarom beter zijn. Criminaliteit moet kunnen worden opgespoord, maar zonder dat de digitale veiligheid van miljoenen andere mensen in gevaar komt.

Bronnen:

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

Chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://open.overheid.nl/documenten/ronl-d497ea5bebe949b3cde930209d87e131413e6b09/pdf

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/

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

NOS Nieuws. (2021, 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. (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

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