Argumentenkaart
Inperking versleuteling

Wat zijn voor Nederland de argumenten voor en tegen een wet die OTT-dienstverleners verplicht communicatie te kunnen ontsleutelen voor opsporingsdiensten?

Voor

Veiligheid

De wet helpt nationale veiligheid waarborgen en (zware) misdrijven voorkomen en opsporen
- Opsporingsdiensten krijgen toegang tot kanalen die voor hen steeds meer relevante informatie bevatten.
- De wet helpt in het bijzonder bij bestrijding van kinderporno, terrorisme en georganiseerde misdaad.
- Opsporing wordt effectiever, omdat er altijd betrouwbare toegang is tot versleutelde communicatie.
- De wet omtmoedigt criminelen en kwaadwillenden, omdat de kans groter is dan nu dat ze gepakt worden.

De wet maakt het waarborgen van de veiligheid goedkoper en efficiënter
- De wet maakt toegang tot versleutelde communicatie goedkoper en sneller dan huidige alternatieven.
- Opsporingsdiensten met beperkte middelen krijgen met de wet óók toegang tot versleutelde communicatie.
- Criminelen zullen zich verplaatsen naar een beperkte set diensten, wat opsporing vereenvoudigt.
- De wet maakt het voor OTT-dienstverleners makkelijker om kanalen te filteren op bijvoorbeeld kinderporno.

Grondrechten

De wet leidt tot gelijke bescherming van grondrechten in het digitale en fysieke domein
- De wet is vergelijkbaar met wetten uit het fysieke domein, zoals uitzonderingen op het briefgeheim.
- Opsporingdiensten zullen transparanter opereren, omdat ze nu vooral geheime methoden gebruiken.
- Osporingsdiensten hebben de wet nodig om in een digitale samenleving criminaliteit te kunnen bestrijden.

De wet leidt tot een meer proportionele inzet van opsporingsmiddelen
- De wet is juridisch en technisch beter te begrenzen dan alternatieven, zoals de hackbevoegdheid.
- De wet is minder ingrijpend dan voorgestelde alternatieven, zoals een verbod op online anonimiteit.
- De wet biedt een alternatief voor huidige methoden die soms de privacy van veel mensen schenden.
- Door de wet hoeven opsporingsdiensten minder (vaak) zware middelen in te zetten, zoals infiltratie.
- Burgers en bedrijven voelen zich door de wet beter beschermd tegen (online) criminaliteit.

Economie

De wet draagt bij aan een gelijk speelveld en innovatie
- OTT-dienstverleners krijgen een verplichting die al geldt voor andere communicatie-dienstverleners
- Bedrijven zullen nieuwe versleutelde diensten proberen te ontwikkelen die niet onder de wet vallen.

Politiek

De wet is politiek aantrekkelijk
- De overheid kan laten zien dat zij stevige maatregelen neemt om zware criminaliteit aan te pakken.
- De overheid kan laten zien dat zij ook grote (technologie)bedrijven kan onderwerpen aan regulering.
- De wet laat zien dat Nederland werk maakt van haar internationale plicht tot opsporing en vervolging.

Tegen

Veiligheid

De wet is niet noodzakelijk voor de opsporing en nationale veiligheid
- Opsporingsdiensten hebben al genoeg manieren om versleuteling te kraken, zoals de hackbevoegdheid.
- Opsporingsdiensten hebben genoeg bevoegdheden, alleen onvoldoende middelen om deze in te zetten.

De wet zal Nederland nauwelijks veiliger maken
- Criminelen zullen overstappen naar versleutelde diensten die niet onder de wet vallen, zoals Encrochat.
- De kans bestaat dat (sommige) OTT-dienstverleners zullen weigeren de wet na te leven.
- Als OTT-dienstverleners zich terugtrekken uit Nederland blijven hun diensten hier (illegaal) beschikbaar.
- Gebruikers zullen onvoorzichtiger zijn met informatie via OTT-kanalen omdat ze zich veiliger wanen.
- Opsporingsdiensten hebben niet genoeg capaciteit om alle informatie die de wet oplevert te benutten.

De wet vormt een veiligheidsrisico voor burgers, vitale sectoren en de overheid
- OTT-diensten worden door de wet kwetsbaarder voor misbruik door criminelen en staten wereldwijd.
- OTT-communicatie van de overheid en vitale sectoren kan makkelijker worden afgetapt door staten.
- Kwetsbaarheden in OTT-diensten maken systemen die hierop voortbouwen onveilig, zoals internetbankieren.

Grondrechten

De wet maakt een disproportionele inbreuk op privacy en vrijheid van meningsuiting
- De wet maakt end-to-end versleuteling onmogelijk, die nu geldt als de beste communicatie-beveiliging.
- Opsporingsdiensten krijgen toegang tot communicatie van veel niet-verdachten, zoals via een groepschat.
- De wet ondermijnt maatschappelijke processen die vertrouwelijkheid vereisen, zoals in de journalistiek.
- Mensen zullen zichzelf meer censureren als ze weten dat de overheid toegang heeft tot hun communicatie.
- De maatschappelijke druk om meer online inhoud te monitoren zal toenemen als het technisch mogelijk is.
- De overheid heeft de alternatieven en hun impact op grondrechten onvoldoende onderzocht en afgewogen.

Bescherming van grondrechten is door de wet moeilijk te waarborgen
- Ook landen zonder stevige rechtstaat zullen OTT-dienstverleners gaan dwingen communicatie te ontsleutelen.
- Landen zullen (rechtmatige) toegang proberen te krijgen tot communicatie van mensen in Nederland.
- Het is juridisch ingewikkeld te bepalen welke landen onder welke voorwaarden de wet mogen gebruiken.
- De wet is een opmaat naar verdere opsporingsmiddelen, zoals het aftappen van andere online diensten.
- Gebruikers van versleutelde diensten die buiten de wet vallen kunnen onterecht als verdacht worden gezien.

Economie

De wet ondergraaft economische ontwikkeling en innovatie
- De wet remt economische activiteit waarvoor geldt dat (vertrouwen in) veilige communicatie noodzakelijk is.
- De wet remt economische activiteit als OTT-dienstverleners zich door de wet terugtrekken uit Nederland.
- De wet kan het gebruik van OTT-diensten verkleinen omdat mensen weten dat de overheid kan meekijken.

De wet benadeelt OTT-dienstverleners
- De wet verplicht OTT-dienstverleners hun diensten onveiliger en dus onaantrekkelijker te maken.
- OTT-dienstverleners moeten systemen aanpassen, wat kosten verhoogt en de kwaliteit onder druk zet.
- Regimes zonder stevige rechtstaat zullen OTT-dienstverleners onder druk zetten hen ook toegang te geven.

Politiek

De wet vormt een politiek afbreukrisico
- De overheid geeft het signaal dat het grondrechten en veilige communicatie niet belangrijk vindt.
- De overheid geeft het signaal dat ze de veiligheid van digitale infrastructuur onvoldoende prioriteit geeft.

De wet getuigt van inconsistent overheidsbeleid
- In 2016 stelde het kabinet juist dat het digitale veiligheid en versleuteling van groot belang vindt.
- Andere wetten, zoals de AVG, verplichten bedrijven juist om informatie maximaal te beveiligen.

Over deze kaart

Deze kaart bevat voor Nederland de argumenten vóór en tegen een wet die over-the-top diensten (OTT-diensten) verplicht om communicatie - op basis van een rechtmatig verzoek – in leesbare vorm beschikbaar te kunnen stellen voor opsporingsdiensten, bijvoorbeeld door deze te ontsleutelen. Uitgangspunt bij deze kaart is dat de wet niet voorschrijft welk mechanisme OTT-dienstverleners moeten gebruiken voor het ontsleutelen van de communicatie. De op deze kaart gebruikte begrippen zijn op de achterzijde van de kaart gedefinieerd, en wijken soms iets af van de gangbare definities.

Aanleiding voor het maken van deze kaart is een wetsvoorstel dat in maart van 2021 door het ministerie van Justitie en Veiligheid is aangekondigd en in een nieuwe kabinetsperiode wordt verwacht. Het wetsvoorstel is een aanvulling op bestaande (digitale) opsporingsmiddelen, zoals de hackbevoegdheid die opsporingsdiensten in bepaalde gevallen het recht geeft op afstand binnen te dringen op geautomatiseerde werken, zoals smartphones en computers.

Deze Argumentenkaart is gemaakt in opdracht van de Amsterdam Internet Exchange (AMS-IX) en het Platform voor de Informatie-Samenleving (ECP), onder leiding van De Argumentenfabriek. Samen met een brede groep experts van bedrijven, overheden, kennisinstellingen en non-gouvermentele organisaties (zie achterzijde voor de namen van deze organisaties) verzamelden we in drie denksessies de argumenten op deze kaart.
We danken allen voor hun denkwerk.

in opdracht van: amsix, ECP Platform voor de InformatieSamenleving

gemaakt door: De ArgumentenFabriek, De Argumentenkaart

Argumentenkaart
Inperking versleuteling

Begrippenlijst
Over-the-top (OTT) diensten/dienstverleners: algemeen beschikbare communicatiediensten die werken via het open internet, en die veelal werken met een door hen zelf (end-to-end) versleutelde verbinding, zoals WhatsApp, Signal, Telegram en iMessage.
Versleuteling (of encryptie): het beveiligen van digitale communicatie met een wiskundige techniek met het doel dat de communicatie alleen door de zender en de door haar of hem beoogde ontvanger(s) te lezen is. Bij versleuteling die niet end-to-end versleuteld is, bestaat de mogelijkheid dat de dienstverlener óók mee kan lezen.
End-to-end versleuteling (of encryptie): versleuteling op een zodanige manier dat de communicatie alléén door de zender en de door haar of hem beoogde ontvanger(s) te lezen is.
Ontsleuteling (of decryptie): het weer leesbaar maken van versleutelde informatie.
Opsporingsdiensten: Opsporings- en veiligheidsdiensten. Opsporingsdiensten zijn overheidsdiensten die belast zijn met het opsporen van criminelen en strafbare feiten, zoals de politie. Veiligheidsdiensten zijn de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD).
Wet: een wettelijke verplichting voor over-the-top diensten OTT-diensten om communicatie – op basis van een rechtmatig verzoek – in leesbare vorm beschikbaar te kunnen stellen voor opsporings- en veiligheidsdiensten, bijvoorbeeld door deze te ontsleutelen.

Betrokken organisaties
Deze kaart kwam tot stand met de hulp van experts van de volgende organisaties:

Agentschap Telecom, Apple, Bits of Freedom, Cyber Security Raad, Europarlement, Expertise Bureau Online Kindermisbruik, Facebook, Fox-IT, IBM, KPN, Microsoft, Ministerie van Buitenlandse Zaken, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Ministerie van Defensie, Ministerie van Economische Zaken en Klimaat, Ministerie van Justitie en Veiligheid, Nederlands Cyber Security Centrum, Nederlands Forensisch Instituut, Northwave, Nederlandse Vereniging van Journalisten, Openbaar Ministerie, Open Future Foundation, Politie Amsterdam, Politie Team High Tech Crime, Radboud University, Safetynet, TU Delft en Universiteit van Amsterdam.

Elke organisatie heeft een eigen perspectief op de argumenten op de kaart, wat betekent dat zij het niet eens hoeven zijn met alle argumenten en de argumenten ook anders zullen wegen.

in opdracht van: amsix ECP Platform voor de InformatieSamenleving