Beschouwing Terrorisme en Privacy

In april 2016 introduceerde WhatsApp een nieuwe technologie, die ervoor moet zorgen dat je berichten veilig zijn en niet in verkeerde handen kunnen vallen. Deze zogenaamde end-to-end encryptie houdt in dat alleen jij en je contact de inhoud van het gesprek kunnen lezen. Deze verandering zorgde voor kopzorgen voor de veiligheidsdiensten, zowel in Nederland als in het buitenland. In september 2016 kwam naar buiten dat de inlichtingendienst AIVD de versleuteling van chatdiensten wil beperken in het kader van terrorismebestrijding. Met dit standpunt staat de AIVD lijnrecht tegenover het Nederlandse kabinet, dat juist voorstander is van het versleutelen van informatie. Vandaag de dag is dit onderwerp het middelpunt van discussie. De vraag die centraal staat is dus wat de prioriteit heeft in de Nederlandse samenleving: privacy of het bestrijden van terrorisme? Het debat over privacy en terrorisme is niet van de ene op de andere dag ontstaan. Na de aanslag op 9 september 2001 heerst er onder de Amerikanen de gedachte dat elke terreuraanslag vermijdbaar is. Hoe? Door te zien wie met wie communiceert. In juni 2013 bracht NSA-klokkenluider Edward Snowden, ex-medewerker van de Amerikaanse inlichtingendienst, verschillende spionageprogramma’s aan het licht. Door middel van deze software kunnen de Amerikanen en de Britten het gedrag van iedere internetgebruiker in de gaten houden.

Sinds hij deze informatie openbaarde, is er wereldwijd een debat losgebarsten over de grenzen van privacy. Door deze discussies zijn technologiebedrijven sterkere versleuteling gaan gebruiken. Hiermee botsen de belangen van de inlichtingendiensten en gebruikers en technologiebedrijven. Zo ontstond er een conflict tussen de Amerikaanse FBI en elektronicabedrijf Apple. De FBI wilde dat Apple de iPhone van een terrorist zou kraken. Apple weigerde dit, omdat daarmee de beveiliging van telefoons van miljoenen mensen in gevaar zouden komen. Het meest recente gevolg van het ‘privacy versus terrorisme’- vraagstuk is het verzoek van de AIVD en de veiligheidsdiensten om de encryptie te beperken.

Nederland heeft laten weten voorlopig niet op te treden tegen informatieversleuteling. Terwijl andere landen juist toegang eisen tot internetgegevens, gaat het kabinet juist investeren in een nog sterkere versleutelde omgeving. Om de privacy en veiligheid van Nederlanders te beschermen, moet dit niet worden verzwakt door een ‘achterdeurtje’. Door dit achterdeurtje zouden opsporingsdiensten toch toegang krijgen tot versleutelde gegevens. "Ter bescherming van de persoonlijke levenssfeer en vertrouwelijke communicatie van overheid en bedrijven is encryptie belangrijk," aldus minister van Veiligheid en Justitie Van der Steur.

Rob Bertholee, hoofd van de inlichtingendienst AIVD, zegt in een reactie op het standpunt van het kabinet: “Dan moet je als regering ook accepteren dat we niet meer bij de communicatie van terroristen kunnen.” Hij is een felle voorstander van inperking van encryptie. “Ik vind bescherming van privacy uitermate belangrijk, maar zou men privacy ook als hoogste doel hebben, als zij slachtoffer zijn van een aanslag?”

Dick Schoof, Nationaal Coördinator Terrorismebestrijding en Veiligheid, zegt dat radicale moslims vaak WhatsApp gebruiken om te communiceren. “Als terroristen via dit soort versleutelde netwerken communiceren, willen we dat wel graag breken. Het is nodig voor de strijd tegen terrorisme en er is goed toezicht op. Door informatieversleuteling is het internet nu een ‘black box’. De diensten moeten daar toegang toe kunnen krijgen.”

Europese antiterreurcoördinator Gilles de Kerchove vindt versleuteling ook een groot probleem voor de veiligheid. Volgens hem moet de Europese Unie overwegen om bedrijven te verplichten versleutelde informatie vrij te geven. De Britse premier Cameron staat hem bij. “Willen we in ons land communicatiemiddelen toestaan die onleesbaar zijn voor ons? Nee, dat moeten we niet doen.”

Toch zijn er mensen die vinden dat privacy zwaarder weegt dan terrorismebestrijding. Zo ook Apple-topman Tim Cook. “Terrorisme is verschrikkelijk en moet gestopt worden. Het opeisen van informatie van gewone burgers en het tegengaan van informatieversleuteling maakt het Westen alleen niet veiliger.” Hij benadrukt dat terroristen ook hun informatie versleutelen en weten wat ze er mee moeten doen. “Als wij gegevens van consumenten niet versleutelen, zijn goede mensen de dupe.”

“Alles afluisteren houdt terrorisme niet tegen,” zegt privacy-expert Mathias Vermeulen. Hij vindt het verzamelen van informatie van onschuldige internetgebruikers problematisch. “Het is inefficiënt en je schendt de privacy van gewone burgers. De samenleving heeft vrijheid nodig. Het geeft een garantie tegen te veel inkijk van de overheid in ons leven. Als de overheid dit wel heeft, zijn kritische ideeën over de samenleving niet mogelijk.”

De meningen over het ‘privacy versus terrorisme’-vraagstuk zijn dus uiteenlopend. Bovendien is het niet alleen een nationaal probleem, ook internationaal gezien wordt er veel aandacht aan het probleem besteed. Het zal dus nog een hele klus worden om een compromis te sluiten. In Nederland is het antwoord op de probleemvraag wél duidelijk. Uit een onderzoek van NUtech.nl blijkt dat de strijd tegen het terrorisme belangrijker is dan totale privacy. 73% van de 2000 respondenten zijn bereid privacyschending te accepteren, als dat helpt om terroristen op te sporen. 18% stelt dat privacy niet geschonden mag worden, ook niet voor terrorismebestrijding. In Nederland is de strijd tussen privacy en de strijd tegen terrorisme dus snel gestreden.