Openingssalvo in nieuwe Nederlandse Crypto Wars?

Opinie

*Ot van Daalen**

Op 3 november 2019 pleitte minister Grapperhaus in *Nieuwsuur* voor een 'sleutelrecht': justitie zou toegang moeten krijgen tot versleutelde chatberichten, als daarmee afbeeldingen van seksueel kindermisbruik worden gedeeld. Hij schaart zich daarmee in een lange lijst beleidsmakers sinds de jaren negentig die sterke encryptie aan banden willen leggen. Geen nieuw idee dus. Maar nog steeds een slecht idee.

Bijna dertig jaar geleden, in 1991, stelde senator Joe Biden al voor aanbieders van communicatiediensten en -apparatuur te verplichten encryptie te ontsleutelen op verzoek van justitie. Het voorstel leidde tot commotie bij activisten, en bij één antikernwapenactivist in het bijzonder. Phil Zimmerman werkte al een paar jaar aan de eerste software die sterke encryptie – encryptie die alleen toegankelijk is voor de gebruiker – voor iedereen beschikbaar zou maken: Pretty Good Privacy, PGP. Hij besloot vóór stemming van het wetsvoorstel, het eerste weekend van juni 1991, zijn programma snel te verspreiden via USENET.

Dat was het begin van de eerste Crypto Wars – de strijd om sterke encryptie. Amerika was niet het enige land dat sterke crypto wilde beperken. Ook Nederland overwoog in 1994 het gebruik van sterke encryptie te reguleren. Een gelekt wetvoorstel (zie *Mediaforum*)[1] leidde tot verontwaardigde reacties en bereikte het parlement niet. In 1997 zei de regering zelfs dat sterke cryptografie niet moet worden beperkt.[2] Nederland stond niet alleen in die koerswijziging: wereldwijd gaven overheden de strijd op. Begin 2000 hadden de voorstanders van sterke encryptie de Crypto Wars gewonnen.

Het Nederlandse standpunt is in 2016 tot officieel beleid verheven, in het "Kabinetsstandpunt encryptie".[3] Grapperhaus' omslag is dan ook opmerkelijk, maar past in een ontwikkeling. Eerder dit jaar lekte uit dat de Duitse regering overwoog de encryptie in WhatsApp te beteugelen – ook daar in strijd met het officiële Duitse standpunt.[4] In Amerika bepleitte Minister van Justitie Barr in oktober 2019 dat het altijd mogelijk moet zijn toegang te krijgen tot versleutelde gegevens.[5]

De vraag blijft dus relevant of het reguleren van sterke encryptie wel kán. Om die te beantwoorden gaan we nog eens naar Zimmerman. Bij de publicatie van PGP legde hij uit waarom encryptie belangrijk is. "*If we do nothing, new technologies will give the government new automatic surveillance capabilities that Stalin could never have dreamed of. The only way to hold the line on privacy in the information age is strong cryptography.*" En: "*PGP empowers people to take their privacy into their own hands. There has been a growing social need for it. That's why I wrote it.*"

Encryptie gaat over macht, en sterke encryptie geeft burgers macht in een wereld van toenemende digitalisering. Op het internet zijn burgers constant voorwerp van surveillance – door overheden, zo weten we uit de Snowden-onthullingen, en door bedrijven, zo leren we door schandalen over techgiganten. Ook buiten het internet laten we een gedetailleerd spoor achter – via telefoons, betalingen, camera's. Ondertussen is de stand van informatiebeveiliging dramatisch: hardware, software, diensten – overal worden kwetsbaarheden gevonden, en sommige kunnen zelfs niet worden gedicht.

En dat is relevant voor een grondrechtelijke analyse van verplichte backdoors. Sterke encryptie biedt een kans de verstoorde machtsverhouding tussen burgers en overheid te herstellen, al is het maar een klein beetje. Het geeft mensen de mogelijkheid onbespied met elkaar te communiceren en hun gegevens veilig op te slaan, zelfs in de cloud. Het maakt het mogelijk voor bedrijven om informatie goed te beveiligen.

Iedere beperking van encryptie – zoals verplichte backdoors – zal aan het grondrechtelijk kader van privacy en communicatievrijheid moeten worden getoetst. Nu het machtsevenwicht verstoord is ten nadele van gebruikers, zal een beperking al snel disproportioneel zijn, maar die conclusie hangt natuurlijk af van de precies voorgestelde maatregel.

Het Hof van Justitie heeft de afgelopen jaren laten zien niet terug te deinzen voor stevige privacybeschermende uitspraken. En sinds het Handvest hebben voorstanders van sterke encryptie bovendien een troefkaart: onder artikel 52 moeten alle beperkingen "de wezenlijke inhoud" van die rechten en vrijheden eerbiedigen, anders kom je niet eens aan de proportionaliteitstoets toe.

Het Hof heeft in *Digital Rights Ireland* en de zaak over het *PNR-verdrag* overwogen dat, nu beveiligingsmaatregelen waren voorgeschreven, de wezenlijke inhoud van het recht op gegevensbescherming onder artikel 8 niet werd geraakt.[6] Met andere woorden: beveiligingsmaatregelen hebben veel te maken met de wezenlijke inhoud van het recht op gegevensbescherming. Encryptie is een van de belangrijkste beveiligingsmaatregelen. Het verzwakken van encryptie kan dus zomaar de kern van het recht op gegevensbescherming raken.

Het is nog te vroeg om te zeggen of Grapperhaus' proefballonnetje het eerste openingssalvo in een nieuwe Crypto War op Nederlands grondgebied is. Maar één ding is zeker: dit keer beschikken voorstanders van encryptie over een stevig grondrechtelijk arsenaal. Het is te hopen dat de regering die grondrechtelijke overwegingen ter harte neemt.

* Mr. O.L. van Daalen is onderzoeker bij het IViR en advocaat te Amsterdam (Root Legal).

1 *Mediaforum* Bijlage 1994 [6]6, p. B49-B55.

2 Zie bijv. *Kamerstukken II* 1997/98, 25 880, nr. 1, p. 158, 162 en *Kamerstukken II* 1998/99, 25 880, nr. 3, p. 2, *Kamerstukken II* 1999/00, 25 880, nr. 10, p. 20.

3 Kamerbrief over kabinetsstandpunt encryptie van 4 januari 2016, te vinden op: http://bit.do/fh5KV.

4 Jörg Diehl et al., 'Horst Seehofer greift WhatsApp an', *Der Spiegel* 2019.

5 Zie speech van Barr van 4 oktober 2019, te vinden op: http://bit.do/fh5JP.

6 HvJ EU 8 april 2014, C-293/12 en C-594/12 (*Digital Rights Ireland*), r.o. 40; HvJ EU 26 juli 2017, Opinie 1/15, r.o. 150.