de jonge wetenschapper
Ilina Georgieva

‘We zouden niet zo makkelijk onze data moeten weggeven’

TEKST: WILKE MARTENS, FOTO: TACO VAN DER EB

Datalekken, cyberaanvallen en hackers: de veiligheid in de virtuele wereld staat onder druk. Steeds meer landen ontwikkelen regelgeving om cyberspace veilig te houden. Maar hoe maak je regels en hoe stel je normen in een internationale digitale werkelijkheid? Jurist Ilina Georgieva (36) onderzoekt de rol van veiligheidsdiensten in cyberspace.

Hebben we alle partijen in het vizier, als we het hebben over normen en regels in cyberspace? Dat is de belangrijkste vraag in het promotieonderzoek van Ilina Georgieva binnen het The Hague Programme for Cyber Norms. 'Mijn focus ligt op veiligheidsdiensten', zegt ze. 'Hoe werkt de macht van een nationale veiligheidsdienst in een internationale en grenzeloze digitale werkelijkheid? Ze spelen namelijk een grote rol, ook al leggen ze voor hun activiteiten nauwelijks verantwoording af. In feite creëren ze normen voor andere internationale spelers in cyberspace.'
Veiligheidsdiensten hebben bijvoorbeeld hun eigen middelen om zero days (zie kader) op te sporen en te bewaren. 'Hiermee kun je veel macht uitoefenen', legt Georgieva uit. 'Veiligheidsdiensten voeren allerlei complexe operaties in cyberspace uit, zonder dat we precies weten wat ze doen. Edward Snowden, de bekende klokkenluider, fungeerde als een belangrijke katalysator. Sinds zijn onthullingen werken veiligheidsdiensten meer aan hun reputatie. Ze vertellen bijvoorbeeld dat ze aanslagen hebben voorkomen. Zo berichtte de Militaire Inlichtingen- en Veiligheidsdienst in 2018 een Russische hack te hebben voorkomen. Dit heeft normatieve consequenties: door de inlichtingendiensten van andere staten aan te spreken op hun gedrag, wordt een scheidslijn getrokken tussen acceptabel en onacceptabel gedrag in cyberspace.'

Online veiligheid

Overheden moeten in dit samenspel actiever worden in regelgeving rondom online en digitale veiligheid. Zij moeten bepalen voor welke normen zij willen staan. 'Onze nationale veiligheids- en inlichtingendiensten maken actief gebruik van data en algoritmes', legt Georgieva uit, 'meestal voor een goed doel, om nationale belangen te beschermen. Maar daardoor komt onze privacy wel onder druk te staan. Dat is een groot goed, dus we moeten continu de balans blijven opmaken.'
Ook de burger heeft een verantwoordelijkheid. 'Iedereen loopt allang met een *tracking device* rond: je smartphone', zegt ze. 'Weinig mensen lezen alle voorwaarden als ze een app installeren en op "akkoord" klikken. Als burger zouden we niet zo makkelijk onze data moeten weggeven. Voor je het weet vindt een algoritme jouw profiel problematisch en beland je op een zwarte lijst.'
Hoewel ze nu meepraat over cyberspace, algoritmes en AI, was Georgieva als kind niet bepaald een techneut. 'Ik ben geboren en opgegroeid in Bulgarije, in een familie van academici', vertelt ze. 'Talen vond ik altijd al leuk en ik leerde graag. Op de middelbare school was ik geïnteresseerd in mensenrechten, antidiscriminatie en menselijke waardigheid. Ook wist ik al vroeg dat ik in het buitenland wilde studeren.'

Activist

Ze hoopt haar kennis uiteindelijk in te zetten voor een rechtvaardiger wereld. 'Die kleine activist van vroeger zit nog altijd in me', lacht ze. 'Voorlopig ben ik heel blij met mijn huidige werk, maar ik hoop ooit concreet te kunnen bijdragen aan een eerlijkere en inclusievere wereld. Misschien kan ik in de toekomst helpen technologie en de voordelen ervan toegankelijker te maken voor vrouwen en meisjes. Ik merk dat het toch nog vaak lastig is als vrouw in tech.'
Ze koos voor een studie Rechten in het Duitse Heidelberg, aangevuld met een jaar Spaans recht in Barcelona en de master Public International Law in Utrecht. Vier jaar geleden solliciteerde ze op de PhD-positie bij het The Hague Programme for Cyber Norms. 'Nederland beviel me goed en eerder had ik onderzoek gedaan naar de preventie van seksueel misbruik op internet', zegt ze, 'dus ik had een link met de digitale wereld. Maar ik moest nog veel leren over de technische aspecten van cyberspace.' ◻

Wat is... een zero day?

Een zogenoemde zero day is een kwetsbaarheid in software die nog niet bekend is bij de ontwikkelaar. De 'zero' verwijst naar het aantal dagen dat de ontwikkelaar de tijd heeft gehad om het probleem op te lossen. Er zijn hackers die expliciet op zoek gaan naar deze zero days. Soms in opdracht van de ontwikkelaar om het systeem te testen, maar meestal voor andere partijen of zichzelf. De zero days zijn namelijk veel geld waard, omdat ze gebruikt kunnen worden voor cyberaanvallen. Er wordt dan ook flink in gehandeld op het dark web. Zodra de zero day bekend is bij de ontwikkelaar, wordt het lek gedicht en het systeem verbeterd. Gebruikers herkennen dat in de vorm van updates.