REDACTIONEEL

Veiligheid in een digitaliserende samenleving

Wouter Stol, Ben Kokkeler, Emile Kolthoff & Robin van Halderen

Veiligheid is de effectieve bescherming van mensen tegen aantasting van hun lichamelijke en geestelijke integriteit. Uitzondering daarop zijn ziekten waarvan geen externe oorzaak bekend is. Die tasten wel de lichamelijke of geestelijke integriteit aan, maar zijn een medisch probleem. Wanneer de medische wetenschap een externe oorzaak identificeert (bijv. asbest, roken, fijnstof), wordt het alsnog een veiligheidsprobleem. Veiligheid is dus een te bereiken status die in de kern bestaat uit het effectief beschermd zijn tegen kwalijke inwerkingen op lichaam en geest.

Digitalisering is een ontwikkeling die inhoudt dat informatie- en communicatietechnologie (ICT), en daarmee dus ook digitale datastromen, op steeds meer plaatsen en op steeds meer manieren een rol spelen in ons dagelijks leven. Digitalisering is niet enkel de productie, verspreiding en ingebruikname van ICT-apparatuur. Het omvat ook de ontwikkeling en verspreiding van een geestelijke gesteldheid die daarbij past: een vorm van rationeel denken die Marcuse in zijn *De eendimensionale mens* (1968) 'techno-logie' heeft genoemd. De term 'technologie' (met koppelteken) verwijst bij Marcuse naar het beredenerend en berekenend denken waarop de moderne techniek is geschoeid en waarmee de leefwereld instrumentalistisch tegemoet wordt getreden. Zo'n denkwijze is onlosmakelijk onderdeel van ons technologisch complex. Illustratief daarvoor is bijvoorbeeld de discussie over de vraag of algoritmen wel of juist niet de basis moeten zijn voor beslissingen die worden gemaakt door bijvoorbeeld de politie of de rechtspraak.

De digitalisering van onze samenleving heeft grote gevolgen. Ze doorbreekt bijvoorbeeld niet zelden bestaande en gevestigde logica's. Daarmee is zij zowel een uitdaging voor gevestigde theorieën aangaande veiligheid als een uitdaging voor de praktijk van veiligheidszorg. Sociale media bijvoorbeeld zijn versnellers voor het uitwisselen van emoties en betekenissen. De massaliteit van 'dataficatie' en de daarmee gepaard gaande nieuwe sociotechnologische dynamieken leveren veel nieuwe vragen op. Veel organisaties, ook in het veiligheidsdomein, hebben moeite met de lastig voorspelbare wijze waarop burgers zich via internet informeren, anderen beïnvloeden en acties op gang brengen, al dan niet legaal. Tegelijk worstelen organisaties in het veiligheidsdomein met de vraag hoe zij zelf de nieuwe technologische mogelijkheden in hun voordeel kunnen benutten.

De titel van dit themanummer 'Veiligheid in een digitaliserende samenleving' verwijst dus naar het effectief beschermen van mensen tegen aantasting van hun lichamelijke en geestelijke integriteit in een samenleving waarin ICT en dus ook techno-logie en nieuwe vormen van sociotechnologische dynamieken op steeds meer plaatsen en op steeds meer manieren een rol spelen in het dagelijks leven. Veiligheid is een van onze grootste maatschappelijke zorgen, naast bijvoorbeeld

gezondheid, ouderenzorg, diversiteit en werkgelegenheid, en dus is de vraag wat digitalisering betekent voor onze veiligheid een van de hoofdvragen waarvoor de digitalisering ons stelt. Eén aspect daarvan is dat digitalisering resulteert in steeds meer verbindingen tussen maatschappelijke gebieden. De vraag is wat dat betekent voor veiligheid en veiligheidszorg. Een ander aspect is dat onze samenleving technologischer wordt en steeds meer tekenen van virtualiteit vertoont, en dat roept de vraag op of oude principes in veiligheid en veiligheidszorg nog wel stand houden. Houdt onze wetgeving bijvoorbeeld de ontwikkelingen wel bij?

Dát digitalisering ingrijpt op onze veiligheid, behoeft geen uitgebreid betoog. Lastiger is het om te schetsen wat de belangrijkste veiligheidsproblemen zijn waarvoor digitalisering ons stelt, waaraan we dus moeten werken, en welke nieuwe kansen er liggen voor samenwerking in de veiligheidssector en bijvoorbeeld ook met het onderwijs. Als we uitgaan van individueel slachtofferschap, komen we vrij snel uit bij vier soorten delicten als belangrijke veiligheidsproblemen in relatie tot digitalisering: hacken, e-fraude, kinderporno en inbreuk op de privacy. Hacken en allerlei vormen van internetoplichting komen veelvuldig voor. Hacken is een basisdelict dat soms het einddoel is, maar vaak juist een opstapje voor een vervolgdelict, zoals datadiefstal of het leeghalen van een bankrekening. E-fraude leidt tot financiële schade, maar kan bijvoorbeeld ook leiden tot verlies aan vertrouwen in de mensheid en in elektronisch zakendoen. Delicten met kinderporno ontlenen hun ernst vooral aan het leed dat de betrokken jongeren wordt aangedaan en de daarmee gepaard gaande maatschappelijke verontwaardiging. Inbreuk op de privacy kent ten gevolge van digitalisering vele nieuwe uitingsvormen. *Function creep* door toenemende koppeling van allerlei databestanden van overheidsinstanties kent inmiddels veel krachtiger pendanten in de private wereld van bestanden van verzekeraars, parkeerbeheerders, en uiteraard de grote internationale platformen zoals Facebook. Een recente vorm is het beïnvloeden van kiezersgedrag door digitale microtargeting waarbij de grenzen van privacy van burgers worden opgezocht en soms overschreden.

Kijken we niet naar individueel slachtofferschap, maar naar het wat abstractere niveau van de samenleving als geheel, dan komen nog enkele andere problemen in beeld. Zo is er het online moeilijk kunnen vaststellen van identiteiten. Dat ligt natuurlijk deels ten grondslag aan e-fraude, maar ook aan identiteitsfraude en het bemoeilijkt overheidstoezicht. Een tweede maatschappelijk probleem is de kwetsbaarheid van de zogenoemde kritische infrastructuur (bijv. nutsvoorzieningen, waterpeilbeheer, hightechindustrie). Dat is deels de macrovariant van het hackenprobleem, maar problemen in de infrastructuur kunnen natuurlijk ook het gevolg zijn van ICT-storingen en gebruikersfouten. In dit verband valt ook te denken aan kwetsbaarheid voor (bedrijfs)spionage. Een ander probleem op macroniveau is het ontstaan van alternatieve monetaire stelsels met cryptocurrency. Omdat overheidstoezicht daarop ontbreekt, is de vraag wat die ontwikkeling betekent voor bijvoorbeeld witwassen van criminele winsten en de vermenging tussen boven- en onderwereld. Bij de macrovraagstukken horen ook internationale kwesties, zoals cyberwarfare, spionage en de balans tussen vrijheid van informatie en overheidsbemoeienis. Als laatste vraagstuk op macroniveau is in het kader van dit themanummer de invloed van digitalisering op de rechtshandhaving relevant.

Tijdschrift voor Veiligheid 2018 (17) 1-2
doi: 10.5553/TvV/187279482018017102001

Opsporingsdiensten worden geconfronteerd met nieuwe vormen van criminaliteit en nieuwe digitale bronnen waaraan zij informatie kunnen onttrekken. De omgang hiermee blijkt niet altijd duidelijk en moet voor een deel nog worden verkend. Niet alleen schuilen hierin risico's voor onze veiligheid, maar ook voor de waarden die ten grondslag liggen aan de rechtsstaat.

Hoe gaan we dit soort nieuwe problemen oplossen, zonder nieuwe kansen op benutting van technologische innovaties te missen? Een vergelijking met het terugdringen van het aantal dodelijke verkeersslachtoffers dringt zich op. In de jaren zeventig van de vorige eeuw vielen er in Nederland in een jaar zo'n 3.000 doden in het verkeer. Tegenwoordig zijn dat er ongeveer 600, ondanks het toegenomen aantal afgelegde kilometers – het resultaat van tientallen jaren collectieve inspanning. Drie lessen volgen uit dit voorbeeld. Ten eerste: het is mogelijk om een groot maatschappelijk veiligheidsprobleem te beheersen. Ten tweede: het maximale succes komt pas na tientallen jaren. Ten derde: succes komt door een combinatie van maatregelen (bijv. wetgeving, handhaving, educatie, infrastructuur, veilig ontwerpen, culturele hervorming) en door inzet van een groot aantal partijen (bijv. overheid, industrie, kennisinstellingen). Bij die combinatie van maatregelen hoort een combinatie van invalshoeken: techniek speelt een rol, maar ook – en soms nog meer – menselijke en culturele factoren. Vermoedelijk gaat de vergelijking met verkeersslachtoffers niet helemaal op, omdat digitalisering een complexere maatschappelijke ontwikkeling is dan de toename van het autoverkeer en omdat in tegenstelling tot het fenomeen dodelijke verkeersslachtoffers, bij het plegen van digitale criminaliteit vaak sprake is van opzettelijk handelen en afscherming van het criminele gedrag, maar dat maakt de lessen niet minder relevant.

Wat betekent dit themanummer in dat geheel? Het is een bijdrage op een route van tientallen jaren waarin we op weg zijn van verwarring en onmacht naar een zekere mate van inzicht en beheersing. Het is een belangrijke bijdrage, want kennis en inzicht ontstaan enkel in een debat dat voortdurend wordt gevoed. Dat geldt zeker bij digitalisering, omdat die ontwikkeling zich in hoog tempo voltrekt. Aan het debat draagt dit themanummer bij. Natuurlijk lukt het niet om met zo'n breed thema als leidraad het volledige spectrum te bestrijken. Toch presenteert dit themanummer interessante bijdragen op diverse van de genoemde hoofdthema's en toont het verschillende invalshoeken.

Het artikel van Stol en Strikwerda gaat over het door de politie op internet vergaren van informatie over burgers en daarmee vooral over de balans tussen opsporing en privacy. De auteurs laten zien dat de digitalisering de politie voor bevoegdheidsvraagstukken stelt en dat de wetgever tracht de wetgeving zo aan te passen, dat politiewerk slagvaardig kan zijn terwijl tegelijkertijd haar optreden is gereguleerd. De auteurs bespreken de nieuwe wetsvoorstellen. In hun bijdrage nemen zij onder meer het standpunt in dat bij het reguleren van politiële informatievergaring op internet, niet alleen gekeken moet worden naar het resultaat van de informatievergaring, maar dat vooral ook het technische middel dat de politie inzet (de tool) onderwerp van regulering moet zijn.

De bijdrage van Vanderveen en Samadi behandelt ook het spanningsveld tussen privacy- en opsporingsbelang vanuit het perspectief van opsporingsberichtgeving.

Het klassieke voorbeeld daarvan is het televisieprogramma 'Opsporing Verzocht', maar vanwege de digitalisering heeft opsporingsberichtgeving ook nieuwe gedaanten en een nieuwe dynamiek. Burgers hebben meer mogelijkheden om zelf via de digitale weg aandacht voor een zaak te vragen. De clou is dat opsporingsberichtgeving als regel inbreuk maakt op het recht op privacy van de verdachte. Ook in dit artikel zien we dat de wetgever met nieuwe wetsvoorstellen inspeelt op de digitalisering. De auteurs pleiten voor een brede maatschappelijke discussie over het gebruik van opsporingsberichtgeving in een digitale samenleving. Ze opperen dat een 'privacy impact assessment' daarbij zou kunnen helpen.

Aan opsporing gaat daderschap vooraf, vaak gecombineerd met slachtofferschap. Bullée, Montaya, Junger en Hartel bespreken in hun bijdrage het fenomeen *social engineering*: een aanvalstechniek waarin een dader misleiding en bedrog gebruikt om doelwitten actief te laten meewerken aan hun slachtofferschap. De auteurs bespreken experimenten die zij hebben uitgevoerd om sociale engineering te doorgronden. Verontrustend is dat social engineering vaak succesvol blijkt en dat doelwitten dus nogal eens meegaan in de opzet van de aanvaller, eens temeer als de aanval is gepersonaliseerd. Hoopgevend is dat preventiemaatregelen effect hebben. Echter, het effect van een preventiemaatregel lijkt geen lang leven beschoren. Hoe kan worden bereikt dat preventiemaatregelen wel langer doorwerken, noteren de auteurs dan ook terecht als belangrijke vraag voor vervolgonderzoek.

Borwell, Jansen en Stol houden de focus op slachtoffers met de vraag in hoeverre e-fraudeslachtoffers speciale persoonlijkheidskenmerken hebben. Wat maakt dat sommige mensen wel ingaan op de tactieken van internetoplichters en anderen niet? Uiteindelijk willen ze beter zicht krijgen op preventiemogelijkheden. De auteurs selecteren slachtoffers van phishing en aankoopfraude uit aangiften bij de politie en voeren een survey uit. Hoewel ook zij op onderdelen pleiten voor vervolgonderzoek, luidt de conclusie dat mensen bij wie de Big Five-scores op de door hen gevonden wijze verschillen van de Nederlandse populatie vatbaarder zijn voor e-fraudeslachtofferschap. Dit lijkt kansen te bieden voor gerichte preventie. Met technieken uit de online marketing kunnen mensen met bepaalde persoonlijkheidskenmerken 'getarget' worden, waarna zij gericht kunnen worden benaderd.

Jong, Leukfeldt en Van de Weijer bestuderen met een vignettenstudie de intentie van cybercrimeslachtoffers om aangifte of melding te doen en welke factoren daarop van invloed zijn. Het type delict en de ernst ervan spelen een rol, hetgeen spoort met eerder onderzoek naar cybercrime en traditionele criminaliteit. Verrassende bevindingen zijn bijvoorbeeld: (1) er is geen verband tussen aangifte- en meldingsbereidheid en attitude tegenover de politie, en (2) respondenten die eerder aangifte deden en daar ontevreden over waren, tonen meer aangiftebereidheid dan respondenten die nog nooit aangifte deden. De auteurs waarschuwen voor de generaliseerbaarheid van hun bevindingen, gezien de samenstelling van hun steekpoef (meer dan 80% van de respondenten is vrouw en studeert rechten). Ook hier is vervolgonderzoek dus opportuun.

Novitzky, Verbeek en Kokkeler nemen noch wetgeving noch slachtoffers, maar in plaats daarvan nieuwe technologie als vertrekpunt, en bespreken daarvan de ethi-

sche kwesties. Concreet bestuderen ze het concept *dual use* in relatie tot drones. Een technologie is dual use indien ze niet alleen ten goede wordt aangewend, maar ook wordt gebruikt voor een onbedoeld en kwaadaardig doel (bijv. onveiligheid veroorzaken). Drones maken deel uit van het militaire complex en worden gebruikt door burgers en veiligheidsorganisaties in het publieke en private domein. Regulering door wetgeving loopt achter. De auteurs benadrukken het belang van een ethische analyse bij de verdere ontwikkeling van, in dit geval, dronetechnologie. Impliciet nodigen de auteurs de lezer uit om de aangereikte ethische criteria ook toe te passen op (alle) technologie voor criminaliteitsbestrijding.
Met deze laatste bijdrage sluit het themanummer in feite af met waar het mee begon: de opdracht om te zoeken naar een balans in de toepassing van nieuwe technologie. Ook de drie 'slachtofferstudies' leveren input die helpt bij het werken aan die opdracht: slachtofferschap van cybercrime kunnen we immers zien als een uiting van een verkeerde balans. Slachtoffers van cybercrime zijn slachtoffers van een kwaadaardige aanwending van technologie en betere kennis daarover kan helpen de balans te herstellen. Dit themanummer dient als bijdrage aan dat proces.