Waarom opkomen voor privacy moed vergt

Kathalijne Buitenweg

(Toespraak tijdens de opening van het Academisch Jaar 2021-22)

"Hartelijk dank voor jullie uitnodiging om vandaag hier te spreken op deze opening van het academisch jaar van de academies voor overheidsjuristen en voor wetgeving.
Met veel plezier las ik op de website dat hier een speciale leerlijn 'Digitalisering' wordt aangeboden. Deze prijkt zelfs helemaal bovenaan het lijstje - al is dat wellicht ingegeven door de logica van de alfabetische volgorde. Hoe dan ook is het winst dat op de academies digitalisering zo duidelijk op het netvlies staat.

In de Tweede Kamer – waar ik tot maart jl deel van mocht uitmaken - is het onderwerp veel te lang verwaarloosd. Net als in veel gemeenten, provincies en op ministeries.
Digitalisering is lang gezien als een zaak voor IT-specialisten. Als iets dat maar beter overgelaten kon worden aan mensen met verstand van bits en bytes. Maar digitalisering doet veel meer dan processen versnellen. Het verandert de machtsverhoudingen in onze samenleving fundamenteel. Na jaren van vooral hoopvolle verwachting over hoe nieuwe technologie onze wereld beter zou maken, worden we steeds vaker geconfronteerd met de keerzijde.
Met de macht van de grote techbedrijven.
Met het tekort aan metalen, en daarmee met nieuwe geopolitieke afhankelijkheden.
Met een steeds ondoorzichtiger overheid die haar besluitvorming vaker op algoritmische uitkomsten baseert.
We zitten midden in een nieuwe industriële revolutie. En in deze omwenteling is het bij uitstek ook jullie taak om te zorgen dat de grote veranderingen door digitale innovatie bijdragen aan het realiseren van mensenrechten – en er geen afbreuk aan doen. Met mijn bijdrage vandaag hoop ik jullie daarvoor verder te motiveren.

Het is wel een lastige taak. Eén van de redenen daarvoor is dat veranderingen gradueel verlopen. Bijvoorbeeld ten aanzien van iets dat velen van jullie ongetwijfeld op zak hebben. Een iPhone. Iemand van jullie?
Deze hier bevat mijn hele leven. Mijn afspraken, email, foto's, bankgegevens, notities. Het is reuze makkelijk - maar ook kwetsbaar.
Vorige maand kondigde Apple aan om iPhones te gaan doorzoeken op kinderporno. Google, Microsoft en Dropbox doen zoiets al jaren. Alles wat opgeslagen is in de Cloud wordt gescand. Maar nu zal, te beginnen in Amerika, op de telefoons zélf software gaan draaien die in de gaten houdt wat voor foto's en video's mensen opslaan.
Na kritiek hierop schreef het machtige techbedrijf: 'We willen er duidelijk over zijn dat deze technologie zich beperkt tot het detecteren van materiaal van seksueel misbruik van kinderen dat is opgeslagen in iCloud, en we zullen niet ingaan op het verzoek van een regering om deze functie uit te breiden.'
Zal het?

Kindermisbruik is zo ontwrichtend en zo'n schending van mensenrechten dat vergaande maatregelen om dit tegen te gaan al snel aanvaardbaar zijn. Misschien deze ook wel. Maar geloven jullie dat het hierbij zal blijven?

Of zal de software op termijn ook ingezet worden om terrorisme tegen te gaan? Of om dissidente geluiden over autoritaire regimes op te sporen? Wordt het op termijn uitgebreid naar geschreven teksten? Naar contacten?
Waar ligt de grens? En wie bepaalt die?

Bedrijven verzamelen steeds meer gegevens over ons en brengen ons steeds nauwkeuriger in kaart. Stap voor stap. Het is een ontwikkeling die in de hand wordt gewerkt doordat het verzamelen, transporteren en opslaan van data heel veel goedkoper is geworden, terwijl de rekenkracht van computers met onvoorstelbare sprongen toeneemt. Het maakt het mogelijk om steeds meer gegevens te combineren en daar – statistische – conclusies uit te trekken. Om gedetailleerde profielen van ons te maken.

Ook de overheid maakt in toenemende mate gebruik van de nieuwe mogelijkheden om het handelen en nalaten van mensen te registeren en zelfs te voorspellen. En hoewel we allemaal weten dat wat mogelijk is niet per definitie wenselijk is, blijkt het lastig om niet alles te doen wat technisch kán.

Kijk naar de camera's boven de snelwegen. Die zijn opgehangen om te registreren wie te hard rijdt, en om deze chauffeurs te kunnen beboeten. Maar toen de camera's er eenmaal waren, werd het aantrekkelijk om ze ook in te zetten voor een ander doel, namelijk het opsporen van gestolen auto's. Inmiddels worden, zonder wettelijke basis, ook foto's genomen van de gezichten van de bestuurders en de bijrijders. Zo'n 350.000 per dag. En het OM maakt er graag gebruik van voor opsporingsdoeleinden. Zoals een woordvoerder het zei: 'Camera's zijn de afgelopen jaren gewoon veel beter geworden. Die ontwikkelen zich als een gek. En dan zijn die beelden er en dan is de neiging die te gebruiken groter.' Zo gaat dat.

De voorbeelden van *function creep* zijn eindeloos. In de publicatie 'Big Data in een vrije en veilige samenleving' laat de Wetenschappelijke Raad voor het Regeringsbeleid zien hoe overheden steeds zwichten voor de verleiding om informatie voor andere doeleinden te gebruiken dan waarvoor het verzameld is. Allemaal uit goede bedoelingen. Want daaraan hoeft echt niemand te twijfelen.

De WRR schrijft: 'Function creep gaat in de regel in kleine incrementele stapjes: er wordt een koppeling gemaakt tussen het ene en het andere systeem, er komt toegang voor een nieuwe organisatie tot deze data, enzovoort. Voor elk van deze stapjes is op dat specifieke moment een politieke rechtvaardiging te geven – effectievere, betere dienstverlening, veiliger – maar het cumulatieve resultaat is vaak veel groter dan de som der delen. Bovendien is het 'eindresultaat' iets waar nooit een serieus politiek debat over is gevoerd.'

In de afgelopen jaren heeft zo'n debat in de Tweede Kamer zeker ontbroken. Het heeft er bijvoorbeeld toe geleid dat SyRI, het Systeem Risico Indicatie dat inmiddels door de rechter verboden is, als een hamerstuk is behandeld. Door SyRI werd het mogelijk om allerlei gegevens te koppelen om fraude sneller op te kunnen sporen. Volgens de Raad van State was er nauwelijks een persoonsgegeven te bedenken dat niet voor verwerking in aanmerking kwam. Maar er kwam geen discussie over de grenzeloosheid van het voorstel. Het leek allemaal zo praktisch, en zo logisch. Want wie wil fraude nu niet maximaal bestrijden? De gevolgen voor privacy, de mogelijkheid dat er een

bias in het systeem of in de toepassing zat, de gevolgen voor sociale ongelijkheid, de ondoorzichtigheid van besluitvorming: ze zijn allemaal niet besproken.

Beetje meer gegevens. Bestaande bestanden koppelen. Kleine stapjes.
Wanneer loop je daarmee de verkeerde richting op?
Het is een vraag die we ons steeds opnieuw moeten stellen. En soms zal het antwoord naar verloop van tijd veranderen. Afhankelijk van mogelijkheden. Afhankelijk van dreigingen.

Om een goede afweging te vergemakkelijken wil ik jullie een paar overwegingen meegeven.
De eerste is dat het belang van privacy voor individuen, maar ook voor de samenleving als geheel, wordt onderschat. Ik ga daar straks dieper op in.
De tweede is dat de digitale oplossingen die een grote inbreuk op privacy tot gevolg hebben al snel aantrekkelijk worden bevonden. Uit een blind vertrouwen. En uit angst. Laat me met dat laatste beginnen.

We leven in een angstige samenleving. Volgens de Duitse socioloog Ulrich Beck hebben mensen steeds meer moeite om goed om te gaan met risico's en tegenslag. Breed heerst het beeld dat mensen zelf verantwoordelijk zijn voor hun geluk en succes, maar daarmee ook voor hun ongeluk en falen. Er zijn minder zekerheden en we worden dagelijks geconfronteerd met ellende en dystopieën. Het maakt mensen bang en op zoek naar zekerheden. Van overheden wordt veel verwacht: niet alleen reactief, maar ook een proactief en preventief optreden. Sociale problemen moeten bij voorkeur worden voorkomen; fraude in de kiem worden gesmoord. We willen orde en veiligheid. Voorspelbaarheid.

In die zoektocht naar beheersbaarheid hebben *slimme* oplossingen al snel een streepje voor.
Want we stellen een enorm vertrouwen in techniek. Een overdreven vertrouwen zelfs. Volgens de Wit-Russische publicist Evgeny Morozov is er daardoor een neiging om voor problemen geen andere oplossing te zien dan 'digitale pleisters'. Die zouden per definitie effectiever én goedkoper zijn.

Een van die pleisters die ik eruit wil lichten zijn 'voorspellende algoritmes'. In de afgelopen jaren zijn steeds meer gemeenten daar gebruik van gaan maken. Bij voorspellende algoritmes wordt een veelheid aan gegevens gecombineerd om profielen te kunnen maken van 'typische fraudeurs' of 'typische slachtoffers'. Vervolgens worden grote groepen mensen langs deze meetlat gelegd. Het leidt tot een ranking op basis van een oplopende risicoscore en dat dient dan weer als input voor nader onderzoek of andere maatregelen. Overheden hopen zo een beter beeld te krijgen van wie slachtoffer dreigt te worden van huiselijk geweld, wie mogelijk denkt aan zelfmoord, wie mogelijk fraudeert of andere vormen van criminaliteit begaat. Ze hopen zo hun financiële middelen zo effectief mogelijk in te zetten.

Profilering vestigt soms terecht de aandacht op mensen die voorheen buiten beeld bleven. Het kan dus wel degelijk van waarde zijn. Maar meestal zijn de verwachtingen wel flink hoger dan de werkelijke opbrengst.
Zo lukte het de gemeente Zaanstad niet om met behulp van big data huiselijk geweld beter te voorspellen of te verklaren. En blijkt uit onderzoek dat het nog maar de vraag is of 'predictive policing' écht effectiever is dan mensenwerk.

Opvallend is dat bij tegenvallende resultaten zelden de stekker uit het project wordt getrokken. Het leidt zelfs vaak niet tot bijstelling van de verwachtingen over de effectiviteit van voorspellende algoritmes. Meestal is het aanleiding om alleen maar méér gegevens te verzamelen. Om het algoritme te voeden met méér data.
Kennelijk zijn we er met z'n allen diep van overtuigd dat de digitale pleisters werken en uiteindelijk altijd beter zijn dan de traditionele manier van beoordelen en ingrijpen.

Met ruimte voor experimenten, voor *trial and error*, is natuurlijk niks mis. En sommige ontwikkelingen hebben nu eenmaal tijd nodig. Dat is het lastige: vooruitgang is een zoektocht. Maar het is wel belangrijk om kritisch te blijven of wat kan en wat niet kan. En ook om te voorkomen dat het vertrouwen in ménsen, en hun professionaliteit, verder wordt aangetast. Want dat is de andere kant van de medaille. Het beoordelingsvermogen van politiemensen, maatschappelijk werkers, docenten wordt steeds minder gewaardeerd. Ook door henzelf overigens.

Zo las ik over een systeem dat de gemeente Dordrecht zou gebruiken om in te schatten wie in de toekomst grote kans heeft om schoolverlater te worden. In dat systeem worden dertien variabelen gewogen, waaronder postcode van de school. Bij jongeren waarvan de seinen in het systeem op rood staan komt de leerplichtambtenaar aan de deur, zelfs al heeft zo'n leerling maar één keertje gespijbeld. Anderen - die misschien veel vaker verstek hebben laten gaan – komen ervan af met een brief. Bij een vraag naar de rechtvaardiging hiervan zei de ambtenaar:
'Dit systeem zit vernuftig in elkaar, het houdt met meer factoren rekening dan een mens zou kunnen. Er komen soms namen van leerlingen uit die nog nooit een dag school hebben gemist. Daar gaan we dan toch maar langs, ook al weten we niet goed waarom.'

De Algemene Verordening Gegevensverwerking regelt heel netjes het recht op een menselijke blik bij besluitvorming. 'Omdat de computer het nu eenmaal zegt' is een antwoord dat formeel niet gegeven mag worden. Maar het voorbeeld van Dordrecht laat zien dat het in de praktijk wel degelijk voorkomt.
Het oordeel van professionals wordt ondergeschikt gemaakt aan het algoritme – soms door henzelf.

Denk ik dan dat mensen beter zijn dan computers? Nou nee. Mensen hebben hun beperkingen. Ze kunnen minder gegevens combineren, en elk mens zit boordevol vooroordelen. Maar het is belangrijk om te erkennen dat computers die beperkingen ook hebben. Het komt aan op het zoeken naar een optimale samenwerking.

Wat zijn nu de valkuilen bij algoritmes? Waarvoor is jullie kritische blik hard nodig?
Allereerst moeten algoritmes natuurlijk goed in elkaar zitten. De formule moet kloppen. Maar het is ook van belang dat het algoritme gevoed worden met de juiste data. Dus niet alleen de data die nu eenmaal makkelijk voorhanden is, of de data die het makkelijkste meetbaar is, maar echt de gegevens die nodig zijn om tot de gevraagde conclusie te komen.
Onderzoek van de Amerikaanse politicologe Virginia Eubanks laat zien dat de resultaten anders tóch nog erg ongelijk kunnen uitpakken. In haar boek *Automating Inequality* geeft ze het voorbeeld van een Amerikaanse overheidsinstelling dat een algoritme ontwikkelde om te kunnen voorspellen in welk gezin mogelijk sprake is van kindermisbruik- of verwaarlozing. De instelling maakte daarvoor gebruik van gegevens die al beschikbaar waren. En daar ging het fout, want dat bleken gegevens over

gezinnen die in het verleden financiële steun hadden aangevraagd. Het waren dus armere gezinnen. Vervolgens concludeerde het algoritme zelf dat een laag inkomen blijkbaar een indicator was van kinderverwaarlozing en -misbruik. Slachtoffers uit gezinnen met een gevulde portemonnee bleven daardoor lange tijd onopgemerkt.

Datasets bevatten *per definitie* keuzes. Ze zijn nooit waardevrij. En als gevolg kunnen bestaande ongelijkheden makkelijk worden versterkt.
Jullie kennen misschien het voorbeeld van Amazon. In 2014 zette Amazon een zelflerend algoritme in voor de werving van nieuw personeel. Het systeem werd gevoed met cv's van mensen die sinds 2004 hadden gesolliciteerd en met de informatie of zij al dan niet waren aangenomen. Een jaar later bleek het systeem vrouwen feilloos uit te sluiten. Blijkbaar maakten vrouwen in het verleden weinig kans op een baan bij Amazon en het algoritme borduurde voort op deze historische data. Het algoritme bestendigde daarmee niet alleen de sociale ongelijkheid, maar vergrootte die zelfs omdat de personeelsmedewerkers dachten dat zij konden vertrouwen in wat zij dachten dat een objectieve uitkomst van het algoritme was.

Het is belangrijk om van deze voorbeelden te leren. Bijvoorbeeld wanneer gemeenten, zoals ik wel eens heb gezien, warmlopen voor veelbelovende algoritmes die zouden kunnen beoordelen welke mensen de meeste kans maken om uit een uitkering te stromen. Let erop! Als ze gevoed worden met ongecorrigeerde historische data bevoordelen deze formules al snel de mensen die uit een groep komen die traditioneel vaker werk vindt. Vrouwen met een migratieachtergrond staan dan al snel op achterstand.

Hoe goed een algoritme ook is, en hoe zorgvuldig de data ook is geselecteerd waarmee het wordt gevoed, toch ziet het altijd maar een deel van de werkelijkheid. Namelijk dat wat is ingevoerd. We hebben dus kritische bouwers nodig. En kritische opdrachtgevers.

Maar we hebben ook kritische toepassers nodig.
Professionals die kunnen en durven afwijken van de geautomatiseerde uitkomsten. Dat lijkt simpel, maar in de praktijk blijkt dat ontzettend moeilijk. Ten eerste twijfel je of je er zelf misschien naast zit. En die twijfel heeft je baas ook al snel, juist vanwege dat culturele vertrouwen in technologie.
Het volgen van een computeruitslag geeft rugdekking, terwijl je bij afwijken zelf vol in de wind staat. Want stel je voor dat de computer aangeeft dat iemand mogelijk slachtoffer wordt van huiselijk geweld of suïcidaal is, en jij ten onrechte niet alle toeters en bellen uit de kast hebt getrokken…

In het verleden is vaak gekozen voor algoritmische besluitvorming als onderdeel van een bezuinigingsronde. Maar dat leidt al snel tot verschraling. Als je het goed wil doen komt het aan op het organiseren van een maximaal samenspel tussen mens en machine. Daarvoor zijn investeringen in technologie nodig, maar evenzeer in het versterken van menskracht, van investeren in vakkennis, en in zorg voor een cultuur van vertrouwen en verantwoordelijkheid. Dit maakt de besluitvorming misschien niet goedkoper, maar wel beter en rechtvaardiger. En misschien op de lange termijn daarmee ook goedkoper.

We moeten de beperkingen van technologie dus realistisch onder ogen zien. Dat is eigenlijk nog het makkelijke deel van het verhaal.

Ingewikkelder wordt het om te bedenken waar de grens ligt wanneer bepaalde technologie wel degelijk heel effectief is, bijvoorbeeld bij het vroegtijdig signaleren van fraude of sociale problemen, maar wél leidt tot grote privacy-inbreuken.
Hoe érg is dat?

Het recht op privacy is een mensenrecht. Vastgelegd in Europese en internationale verdragen, en in Artikel 10 van onze Grondwet.
Het idee achter mensenrechten is dat iedereen het recht heeft om zijn of haar leven zelf vorm te geven.
Voldoende privacy helpt bij het kunnen zijn wie we willen zijn. Het maakt het mogelijk om jezelf op een bepaalde manier te laten zien aan vrienden, maar je op een andere manier te presenteren op je werk. Of om je verder te ontwikkelen, zonder steeds achtervolgd te worden door fouten en keuzes uit het verleden.
Privacy beschermt ons ook. Bijvoorbeeld tegen een overheid die teveel in wil grijpen in de levens van zijn burgers. Of tegen criminelen. Cybercriminaliteit is de snelst groeiende vorm van misdaad tegenwoordig, en gedijt bij rondslingerende persoonsgegevens.

Privacy is geen absoluut recht. Er mogen inbreuken op worden gemaakt, maar die moeten wel noodzakelijk, proportioneel en effectief zijn – en ze moeten in een wet zijn verankerd.
Kernbegrippen die daaruit voortvloeien en die nodig zijn bij het overeind houden van zoveel mogelijk privacy zijn ‘dataminimalisatie’ en ‘doelbinding’. Er mogen niet meer gegevens worden verzameld dan nodig is om het doel te behalen en ze mogen alleen worden gebruikt voor het doel waarvoor ze zijn verzameld. Dat klinkt overzichtelijk.

Het lastige van deze principes in de moderne tijd is dat de grootste beloftes van big data daarmee op gespannen voet staan. Juist als algoritmes gevoed worden met heel veel verschillende gegevens, die voor allerlei verschillende doelen verzameld waren, kunnen ze tot onverwachte inzichten komen. Denk aan de dertien variabelen van de gemeente Dordrecht.

Vanwege de kansen die big data bieden zie je langzaam de neiging ontstaan om doelbinding een nieuwe interpretatie te geven. Dat kwam goed naar voren afgelopen december in een debat tussen D66 Kamerlid Kees Verhoeven en de minister van Justitie en Veiligheid Ferd Grapperhaus over de Wet gegevensverwerking door samenwerkingsverbanden. Deze wet, die in de volksmond ook wel superSyRI wordt genoemd, maakt het mogelijk dat allerlei organisaties, denk aan gemeenten, politie, energiebedrijven en ook private partijen, de gegevens die zij hebben verzameld voor een bepaald doel, in dat samenwerkingsverband samenbrengen en verwerken voor een nieuw doel.
Kees Verhoeven zei daarover, ik citeer: ‘Hoe kun je nou zeggen dat doelbinding overeind blijft als vele tientallen organisaties met allemaal verschillende doelen die in één breder doel samenkomen, allerlei databestanden mogen gaan uitwisselen binnen hun verband? Hoe kan het dat je vervolgens zegt: ja, dat mag wel, zelfs als het niet verenigbaar is met het doel waarvoor die data ooit verzameld zijn?’
Het antwoord van minister Grapperhaus laat de schuif zien die gaande is: ja, het klopt dat de gegevens voor een ander doel worden gebruikt dan waarvoor ze waren verzameld, maar doordat er nu in een nieuwe wet een nieuw doel wordt vastgelegd wordt toch voldaan aan het principe van doelbinding.

Deze wet zal in de komende jaren nog veel besproken worden. Hoeveel gegevens mogen worden verzameld en verwerkt? Kan het ook onze sociale media omvatten? Hoe gaat de samenwerking zijn tussen overheden en private partijen? Langs welke profielen en meetlatten worden wij allemaal gelegd? En hoe bepalend worden conclusies op grond van statistiek?
Potentieel is de wet heel ingrijpend. En juist omdat veel zaken moeten worden uitgewerkt in amvb's in de kans reëel dat dit weer zo'n voorbeeld is van wat de WRR ons voorhield. Waarbij incrementeel kleine stapjes worden gezet, stuk voor stuk begrijpelijk, maar dat we uiteindelijk zitten met een systeem waarvan de som groter is dan de delen.

Er wordt steeds meer informatie over ons verzameld, gecombineerd en geanalyseerd. Niet alleen door de overheid, maar ook – juist ook – door bedrijven. Er wordt amechtig jacht gemaakt op alles wat we bewust of onbewust prijsgeven. Welke boodschappen we doen, waar we lopen en rijden, wat we lezen, schrijven en met wie we bellen. Onze werkprestaties, schoolresultaten en gezondheidsgegevens. Het wordt allemaal tot data gemaakt en verwerkt.

Er wordt gedaan alsof mensen met goede bedoelingen maar weinig privacy nodig hebben. Zo zei Eric Schmidt, de voormalig topman van Google, ooit: 'Als je iets doet waarvan je niet wilt dat anderen het weten, kun je het misschien maar beter helemaal niet doen.'

Maar het is hoog tijd dat we beter nadenken over de gevolgen van de dataverzameldrift voor onze samenleving als geheel. Want privacy is niet alleen een individueel recht. Het is ook een publiek goed. Iets dat nodig is om de vrije samenleving overeind te houden.

Denk bijvoorbeeld aan onze democratie. Hoe meer informatie over ons bekend is, hoe preciezer politieke partijen hun boodschap op ons kunnen toesnijden: microtargetting heet dat. Het opent de weg niet simpelweg naar verleiding, maar naar regelrechte misleiding en manipulatie.
Het leidt ook tot verbrokkeling van de publieke sfeer. Want wat jullie te zien krijgen ten tijde van verkiezingen is dan heel anders dan wat andere groepen burgers zien. Daarmee doet het ook afbreuk aan onze keuzevrijheid en zelfbeschikking.

De dataverzameldrift, waar je bent, met wie je afspreekt, je zoekfuncties op internet, al die informatie heeft ook gevolgen voor de persvrijheid. We zien het al in de Verenigde Staten. Sinds de onthullingen van Snowden zijn veel bronnen opgedroogd. Mensen voelen zich minder vrij om journalisten over misstanden te tippen omdat ze bang zijn dat informatie herleidbaar is.
De angst (of in sommige gevallen de wetenschap) dat de overheid of anderen meelezen leidt ook tot zelfcensuur. Het heeft een chilling-effect.
De komende jaren zal de aanwezigheid van camera's alleen maar toenemen. Beveiligingscamera's, deurbelcamera's, dashboardcamera's, scanauto's, drones. In combinatie met gezichtsherkenningssoftware worden wij steeds doorzichtiger.
Dat kan de vitaliteit van onze samenleving aantasten. Want een zich steeds vernieuwende cultuur heeft juist onverwachte ontmoetingen nodig, botsende denkbeelden en dwarsdenkers.
Filosoof Miriam Rasch, verwoorde het mooi in haar boek *Frictie – Ethiek in tijden van dataïsme*

‘Als alles is gedataficeerd, alle frictie is uitgebannen en elke beweging langs bekende patronen verloopt, dan komt de wereld tot staan. Een totaal voorspelbare toekomst is geen toekomst, maar een voortdurend heden.

En dan heb ik het nog niet eens gehad over het gevaar voor institutionele discriminatie. Dat mensen op basis van kenmerken, en het tot een bepaalde groep behoren, vaker op het netvlies van de overheid komen. Dat dit sociale ongelijkheid en wantrouwen in de hand werkt. Dat zij zich daarmee ook juist onvrijer voelen. Onveiliger.

Privacy is daarom niet alleen een individueel recht, maar ook een publiek goed. Het is een voorwaarde voor veel andere rechten, van het kiesrecht tot het recht op gelijke behandeling.

We moeten privacy dus herwaarderen – voor een vrije, veerkrachtige samenleving.
Het lastige alleen is dat het belang van privacy zo abstract is. Dat hebben jullie de laatste tien minuten wel gemerkt! En dat terwijl de dreigingen, van de georganiseerde misdaad tot suïcide onder kinderen, heel concreet zijn, net als de technologische oplossingen om die dreigingen tegen te gaan. Het lastige is ook dat er geen duidelijke grens is. Niet elke inbreuk op privacy is problematisch.

En zo is de makkelijkste weg om het volgende kleine stapje te zetten. Stap voor stap.
Het vraagt moed om op te komen voor privacy. Je haalt je wat op de hals als je oog wil hebben voor de weg waarheen die leidt. Om jullie daarin toch aan te moedigen citeer ik graag Evgeny Morozov. Hij inspireerde mij toen hij zei:
‘Soms zullen we meer risico, imperfectie, improvisatie en ondoelmatigheid moeten aanvaarden om de democratische geest levend te houden.’

Dat klinkt voor sommigen als vloeken in de kerk. Toch is dat wat ik jullie wens. Dat jullie hier bij de academie voor wetgeving en de academie voor overheidsjuristen niet alleen leren over hoe jullie kunnen bijdragen aan een overheid die effectief en efficiënt functioneert. Maar ook nadenken over wanneer controle uitmondt in onvrijheid en ongelijkheid. En hoe we er samen voor kunnen zorgen dat technologie geen afbreuk doet aan mensenrechten, maar daaraan bijdragen.

Ik wens jullie veel succes, en bovenal veel plezier.”