Horizontale privacy: een kwestie van vertrouwen?

Esther Keymolen, Universiteit Leiden[1]

Vorig jaar werd in de luchthaven van Colorado een foto gemaakt van Molly Lensing.[2] Op deze foto zie je haar staren naar het scherm van haar smartphone, ogenschijnlijk geen interesse tonend in haar baby die op de grond ligt. Vergezeld van het commentaar *"Albert Einstein said, "I fear the day that technology will take on our humanity… the world will be populated by a generation of idiots"* wordt de foto, zonder Lensings toestemming, op Facebook gepost en gaat vervolgens viral. Duizenden mensen geven commentaar. Sommigen verdedigen de vrouw, maar velen vinden het nodig haar als een slechte moeder te bestempelen.

Door alle heisa voelt Lensing zich tenslotte genoodzaakt te reageren[3]. In een interview legt ze niet alleen uit wat de context van de foto is (haar vlucht was al 20 uur vertraagd. Haar dochter moest even wat bewegingsruimte hebben, terwijl zij via haar smartphone haar familie informeerde over de vertraging), maar vertelt ze ook wat voor impact deze virale foto op haar leven heeft.

Ze geeft aan het te ervaren als een inbreuk op haar privacy. Ze is bang dat haar collega's de foto zien en zullen geloven dat ze geen goede ouder is. Aangezien ze als verpleegster op de kinderafdeling van het ziekenhuis werkt, staat er voor haar ook professioneel wat op het spel. Nog steeds doet de foto online de ronde en wanneer er een nieuwe golf van commentaar verschijnt, probeert ze dit zo goed en zo kwaad als dat kan te negeren en zoekt ze steun bij vertrouwelingen.

[1] Met dank aan Pieter Kalis voor de gedachtenwisseling
[2] http://www.mommyish.com/wp-content/uploads/2017/09/viral-photo-baby-airport-floor.jpg
[3] https://www.today.com/parents/mom-shamed-photo-her-her-baby-airport-t116843.

Waar grootschalige privacyschendingen door bijvoorbeeld datalekken en hacks bij bedrijven en overheden bijna dagelijks de krant (ont)sieren, blijven horizontale privacy-schendingen zoals hierboven geschetst al te vaak onderbelicht. De impact op het leven van betrokken personen is er echter niet minder groot om. Hoewel vanuit reguleringsoogpunt het reeds aanwezig wettelijk kader voor privacy- en gegevensbescherming natuurlijk onmisbaar is en ook de normerende werking van zo'n kader in sociale interacties niet onderschat mag worden, is het voor horizontale privacyvraagstukken misschien niet het allereerste aanknopingspunt. Regulering van privacy in brede zin vindt, behalve door middel van recht, ook in andere domeinen plaats, met name in de sociale interactie zelf.

Horizontale privacy, dus privacy op het interpersoonlijk niveau, is namelijk onlosmakelijk verbonden met vertrouwen in de ander. Privacy als in jezelf onbespied wanen, vrij zijn van de inmenging van derden, of als de mogelijkheid om geheimen te hebben en houden, is niet iets wat door de band genomen afgedwongen kan worden in het sociaal verkeer. Je hebt er de medewerking van de ander voor nodig. Je vertrouwt erop dat je gesprekken tijdens het buurtfeest niet worden opgenomen en dat je foto niet zomaar door een vreemde op Facebook wordt geplaatst. Het is niet iets dat je voortdurend controleert. Je gaat ervan uit dat de mensen om je heen je privacy niet schenden, maar zeker weten doe je het niet.

Dit vertrouwen in de ander om je privacy niet te schenden berust in eerste instantie op gedeelde waarden en normen die zich vertalen in tal van privacy-patronen. Zo houden we een bepaalde afstand ten opzichte van elkaar in de publieke ruimte, vragen we onze baas niet naar de intieme details van zijn liefdesleven noch eisen we van de dokter dat zij haar medische gegevens met ons deelt terwijl we dat wel met haar doen. Deze privacy-patronen werken meestal op de achtergrond en trekken niet onze aandacht. Maar juist het feit dát we deze privacy-patronen achteloos volgen maakt ze zo effectief. Het maakt het gedrag van anderen voorspelbaarder en daardoor gemakkelijker om erop te vertrouwen dat je privacy in goede handen is.

Echter, de mogelijkheden die de huidige technologie biedt om informatie vast te leggen en te delen, stelt deze privacy-patronen, en bijgevolg het vertrouwen tussen burgers, op de proef. Smartphones, apps, social media en meer zijn er op ingericht om zeer gemakkelijk informatie vast te leggen en te delen. Dit is niet louter een

efficiëntieslag maar het beïnvloedt ook de perceptie van wat privacy inhoudt en hoe daar naar te handelen. Zo kunnen burgers slecht inschatten hoe groot het publiek is dat ze bereiken wanneer ze een bericht of foto online posten. Waar het er op het scherm allemaal zeer overzichtelijk uitziet, gaat er achter het scherm een netwerk van actoren schuil dat aan het oog van de burger is onttrokken. Ook het ontbreken van "face-to-face interaction" maakt dat het niet altijd duidelijk is wat de impact van de horizontale privacyschending voor het slachtoffer inhoudt. De technologie stelt ons dus voor de uitdaging privacy in het sociale verkeer te herijken. Ik heb geen pasklare antwoorden voor de vraag hoe dit proces vorm te geven, maar er zijn twee richtingen waaraan ik denk als het gaat om de rol die beleid hierin zou kunnen spelen.

Ten eerste zou er gedacht kunnen worden aan voorlichting. Net zoals de BOB en anti-roken campagnes inzetten op gedragsverandering en op het bestendigen van een bepaalde –morele- standaard in de maatschappij, zou dit misschien ook kunnen werken voor privacy-patronen. Bepaalde *do's and don'ts* op privacy-gebied moeten inslijten zodanig dat burgers erop kunnen vertrouwen dat er sprake is van een gedeeld privacyperspectief.

Ten tweede zou er ook gekeken kunnen worden naar het ontwerp van de technologie zelf. Privacyschendingen tussen burgers onderling kunnen niet los gezien worden van de apparaten en diensten die ze daarvoor gebruiken. De manier waarop de interface wordt ontworpen bepaalt mede de privacy-perceptie van burgers. Zo zou er ingezet kunnen worden op het veel inzichtelijker maken van wie er bereikt wordt met een bepaald bericht; burgers zouden gewaarschuwd kunnen worden door de technologie zelf wanneer met een bepaalde handeling privacy mogelijkerwijs in het geding is[4]. Dat er mogelijkheden zijn om in te grijpen op het ontwerp van diensten en apps laat de AVG (Artikel 25) zien met de vereiste 'Gegevensbescherming door ontwerp en door standaardinstellingen'. Dit behelst onder meer dat de standaard privacy instellingen bij het openen van een social media account automatisch zijn ingesteld volgens de meeste stringente optie. Dit moet ervoor zorgen dat burgers niet onbedoeld informatie delen met een oneindig aantal anderen.

[4] enigszins analoog aan het signaal dat afgaat in de auto wanneer de gordel niet om is.

Het waarborgen van privacy in relaties tussen burgers berust in belangrijke mate op het wederzijds vertrouwen dat privacybelangen over en weer ter harte worden genomen. Dit vertrouwen is belangrijk voor een florerende samenleving waarbinnen burgers zich vrijelijk kunnen bewegen en door technologie bemiddelde interacties kunnen aangaan zonder dat zij van te voren alles moeten overzien, controleren en afdwingen (als dat al mogelijk zou zijn). Wanneer de privacy-patronen die het sociale verkeer mede in goede banen leiden onder druk komen te staan, wordt het moeilijker om dit vertrouwen te schenken. Het ervaren risico wordt dan simpelweg te groot. Dit kan ertoe leiden dat mensen zich belemmerd voelen in hun handelen en bovendien zullen moeten investeren in andere –kostbare- strategieën om meer controle en zekerheid te verkrijgen over hoe anderen met hun privacy omgaan.