Input voor discussie over horizontale privacy

*Bert-Jaap Koops, hoogleraar regulering van technologie bij TILT, Tilburg University
4 oktober 2017*

Dit rondetafelgesprek is zeer welkom: hiermee wordt een belangrijk, onderbelicht thema geagen­deerd, dat veel discussie, reflectie en beleid behoeft. Voor mij komt het thema het meest pregnant naar voren in **gezichtsherkenning**. De technologie ontwikkelt zich dermate snel dat deze nu al wordt toegepast (bijvoorbeeld bij cameratoezicht in Moskou en geldautomaten in China) en naar ik verwacht binnen een paar jaar ook bij ons op de markt zal zijn, in velerlei toepassingen. Winkels en organisaties zullen het kunnen gebruiken om herhaalklanten te herkennen en dienst­verlening te personaliseren (en nog meer data te verzamelen dan nu al met bijvoorbeeld WiFi-tracking gebeurt). Denkbaar is dat binnen 5-10 jaar iedereen apps kan binnenhalen waarmee de smartphone omstanders kan herkennen – en het is vooral deze ontwikkeling die mij zorgen baart.

Op straat, in de trein en in het café ben je tot nu toe, in de praktijk, behoorlijk **anoniem**; je kunt herkend worden, maar dat gebeurt – in grootstedelijke omgevingen – bij hoge uitzondering, zeker als je buiten je directe woon- of werkomgeving bent. Het betekent dat je in deze ruimten tamelijk onbevangen jezelf kunt zijn (ook met het huidige hoge niveau van cameratoezicht; er moet immers veel moeite worden gedaan om een persoon op een beeld te identificeren), en je ook bijvoor­beeld anders kunt kleden of gedragen dan je op je werk of bij kennissen zou doen. Dit verandert radicaal wanneer je door iedereen overal herkend kunt worden. Enerzijds is iedereen plotseling een bekende Nederlander als ieder ander je kan identificeren en automatisch kan Googelen, en anderzijds loop je altijd het risico dat iemand (ook ongemerkt) een foto van je maakt – in korte broek, gapend of met volle mond, of in welke pose dan ook waarin je je niet graag presenteert aan je eigen omgeving – en die op Internet plaatst met een automatische herkenning van je identiteit. Wanneer iedereen een gezichtsherkenningsapp op de smartphone kan gebruiken, heb je nergens in de publieke ruimte, maar ook niet in publiek toegankelijke plaatsen als cafés en trein, meer het gevoel dat je onbevangen jezelf kunt zijn, dat tot nu toe een belangrijk onderdeel uitmaakt van het rondlopen in een (groot)stedelijke omgeving met *de facto* anoni­miteit. Gezichts­herkenning zal dan ook een **grote impact hebben sociale omgang**(**svor­men**) in (semi-)publieke ruimten. Zonder tijdig beleid of regulering, zullen dergelijke apps ons gaan overvallen: pas wanneer ze op enige schaal gebruikt worden en mensen de gevolgen van continue herkenbaarheid ervaren, zal er debat ontstaan; maar in dat stadium zijn er weinig knop­pen meer waaraan je kunt draaien om het verlies van anonimiteit en privacy nog te kunnen opvangen.

Dit betekent dat **nu** **het debat** over gezichtsherkenning (en breder over horizontale surveillance-toepassingen, zoals opnemen van gesprekken, emotiedetectie, en het op sociale media plaatsen van beelden zonder toestemming) moet worden gevoerd, en dat **op redelijk korte termijn beleid nodig is** om ervoor te zorgen dat niet iedereen overal en ongebreideld gezichtsherkenning kan toepassen. Ik heb helaas geen oplossingen of concrete beleidssuggesties voorhanden; het is een complex probleem, onder andere door de internationale context van smartphone-ecosystemen, en er zijn geen pasklare antwoorden. Wel wil ik benadrukken dat beleid en regulering zich niet moet beperken tot wetgeving, die waarschijnlijk wel nodig maar niet voldoende is. In recent onderzoek kom ik tot de conclusie dat privacy van oudsher niet primair door het recht wordt geregeld, maar door **sociale normen**;[[1]](#footnote-1) we zijn ons daarvan niet zo bewust, omdat veel sociale normen vanzelfsprekend zijn (je gaat niet te dichtbij iemand staan in de lift als er plaats genoeg is; je vraagt iemand tegenover je in de trein niet naar zijn seksleven; enz.). Een van de kernproblemen van vraagstukken rond digitale privacy – en dus ook spelend bij horizontale privacy in relatie tot technische ontwikkelingen – is dat Internet, smartphones, gezichtsherkenning en dergelijke zich sneller ontwikkelen dan de sociale normen die met het gebruik ervan gepaard gaan. Daarom zijn beleid en regulering nodig, om gedrag bij te sturen dat nog niet wordt ingegeven door een ingesleten normbesef van het effect dat jouw handelen heeft op het leven van anderen.

In reactie op de rondgestuurde *Informele schets* ter voorbereiding van dit gesprek, geef ik nog enkele punten mee ter overweging. Horizontale privacy is niet alleen belangrijk in relaties tussen burgers onderling, maar ook tussen consumenten en **(lokale) bedrijven**. Privacyvraagstukken rond Google, Facebook en andere megamultinationals zijn van een andere orde en horen niet in dit debat thuis; maar privacyvraagstukken rond, bijvoorbeeld, WiFi-tracking door winkels wel.

Het **recht op vergetelheid** is een interessant en belangrijk aanknopingspunt om verspreiding van persoonlijke informatie op Internet tegen te gaan. Potentieel kan het een deel van de problemen helpen oplossen, maar met moet beseffen dat het niet werkt voor een bepaald type probleem: het fenomeen dat sommige informatie, met name foto’s en filmpjes, viraal gaat, en binnen korte tijd veel bekeken en gekopieerd wordt; die informatie duikt (steeds weer) op veel verschillende plaatsen op, en een recht op vergetelheid is dan dweilen met de kraan open.[[2]](#footnote-2) Er moet dus ook worden nagedacht over andere sturingsinstrumenten om verspreiding van informatie tegen te gaan en om de gevolgen van verspreiding te verzachten.

Welke vorm van regulering ook wordt gekozen, veelal zal de uitdaging vooral zitten in handhaafbaarheid en **feitelijke handhaving**. Toezichthouders, waaronder de Autoriteit Persoonsgegevens en de Autoriteit Consument & Markt, zullen voldoende toegerust moeten worden om horizontale privacy te waarborgen; daarvoor is niet alleen investering in kennis nodig, maar vooral ook in **capaciteit**.

Tot slot wijs ik er nog op dat **privacy veel meer is dan** alleen de verwerking van **persoons­gegevens**. Het debat wordt vaak versmald tot data en dataprotectie, maar privacy heeft ook te maken met onbevangen jezelf kunnen zijn voor wat betreft je lichaam, intieme relaties, fysieke omgeving en dergelijke. Dit wordt geïllustreerd in het schema dat mijn collega’s en ik hebben ontwikkeld, dat aangeeft dat informationele privacy weliswaar vaak een rol speelt, maar meestal in relatie tot andere privacyaspecten die niet te reduceren zijn tot de data die worden verwerkt. Een privacydebat en -beleid moet dus niet alleen over data gaan, maar over alle privacyaspecten.



Figuur 1. Typologie van privacy. Bron: B.J. Koops, B.C. Newell, T. Timan, I. Škorvánek, T. Chokrevski & M. Galič (2017), ‘A Typology of Privacy’, 38 Univ. of Pennsylvania J. of International Law, p. 483-575, [https://ssrn.com/abstract=2754043](https://ssrn.com/abstract%3D2754043).

1. B.J. Koops, *Privacy Spaces* (te verschijnen, concept opvraagbaar bij de auteur). [↑](#footnote-ref-1)
2. Dit punt ontleen ik aan het onderzoek van Paulan Korenhof, die in Tilburg een proefschrift afrondt over het recht op vergetelheid. [↑](#footnote-ref-2)