Vrijheid op het internet

Simone van der Hof

Openingscollege voor het facultaire jaar 2014/2015, Hooglandse Kerk te Leiden

Beste studenten, ouders van studenten, collega's, en andere aanwezigen,

In 2009 kreeg het Citizen Lab, een onderzoeksgroep van de Universiteit van Toronto in Canada, een intrigerende onderzoeksopdracht. Het onderzoek dat bekend staat onder de naam Ghostnet leest als een spannende spionageroman uit de 21ste eeuw. Het begon allemaal met verdenkingen van de Tibetaanse overheid dat kantoren van de Dalai Lama in Dharamsala, Noord-India maar ook elders ter wereld digitaal in de gaten werden gehouden door hackers die zich vanuit China toegang zouden hebben verschaft tot de computers van de in ballingschap levende Tibetaanse gemeenschap. Iedere keer dat personen die zich actief inzetten voor de Tibetaanse kwestie China bezochten werden ze vastgehouden en ondervraagd bij de grens en werd duidelijk dat de Chinese autoriteiten toegang hadden tot hun privé e-mails en chatberichten. Ook bleken niet-openbare reisschema's van de Dalai Lama in handen van de Chinezen te zijn gevallen, nadat buitenlandse mogendheden onder druk waren gezet om bezoeken van de Dalai Lama af te gelasten. De Canadese onderzoeksgroep kreeg opmerkelijk genoeg onbeperkte toegang tot computers op kantoren van de geestelijk leider van de Tibetanen om te onderzoeken wat er aan de hand was. Al gauw bleken niet alleen deze computers, maar ook die van ministeries en ambassades in Azië, het Midden-Oosten en Europa gecompromitteerd te zijn door de vanuit China opererende hackers. Saillant detail was overigens dat de Canadese onderzoekers maandenlang ongemerkt al het doen en laten van de hackers minutieus konden volgen, omdat zij hun eigen infrastructuur niet hadden beveiligd. Sterker nog, door een simpele zoekopdracht in Google hadden ze toegang gekregen tot het systeem. Je zou verwachten dat cyberspionnen zelf extra voorzichtig zijn als het gaat om hun cyberveiligheid, een wetmatigheid is dat echter zeker niet. Maar dat terzijde.

De Dalai Lama bevindt zich wel in een heel bijzondere, politiek zeer gevoelige positie, zo zult u nu wellicht denken, en het is dan ook, ofschoon moreel verwerpelijk, toch niet geheel verrassend dat hij, zijn medewerkers en volgelingen slachtoffer worden van hackers die vanuit een hen niet vriendelijk gezinde mogendheid opereren. In zekere zin zitten wij echter allen in de positie van de Dalai Lama. Ook wij, u en ik, worden namelijk — net als de Dalai Lama door de hackers en de hackers vervolgens door de Canadese onderzoekers — continu gevolgd wanneer we online zijn. En

online zijn we steeds vaker en langer met steeds meer mensen, nu het aantal internetgebruikers in de wereld razendsnel stijgt. Steeds meer mensen zijn zelfs 24 uur per dag, 7 dagen per week bereikbaar via de onafscheidelijke smartphone, die dienst doet als ons persoonlijke controleapparaat en al onze online en offline bewegingen kan registreren en delen met anderen. En dat in veel gevallen ook doet. In 2012 had ongeveer 60% van de Nederlanders een smartphone en we mogen gevoegelijk aannemen dat dit percentage inmiddels verder is toegenomen. We zijn enorm afhankelijk geworden van digitale netwerken en de bijbehorende gadgets. De ontwikkeling van digitale technologieën dendert in een sneltreinvaart voort en verandert de samenleving al sluipenderwijs héél fundamenteel. We doen wellicht nog wat lacherig over de onbeholpen ogende Google Glass, maar 'augmented reality' — het projecteren van digitale informatie op de offline wereld — en het volledig versmelten van online en offline door allerlei 'waerables' — draagbare gadgets — wordt de norm. Fysieke objecten, waaronder auto's, fotocamera's, wasmachines en elektriciteitsmeters, worden verbonden met het internet, het zogeheten internet der dingen, en delen informatie, waaronder onze persoonlijke gegevens, met anderen. Het zal u niet verbazen dat er steeds grotere hoeveelheden, gevarieerdere en zeer gedetailleerde persoonsgegevens worden gegenereerd over u en mij en voor een belangrijk deel ook dóór onszelf. Deze data belanden in slimme digitale profielen die de basis vormen voor beslissingen van bedrijven en overheden die ons leven raken. Zal de ziektekostenverzekeraar iemand met een ongezonde levensstijl nog een polis toekennen? Of doet hij dat alleen nog tegen beduidend hogere poliskosten? En wat is een ongezonde levensstijl? Wie bepaalt dat en hoe? De nieuwe autoverzekering Fairzekering monitort continu je rijgedrag om zo de verzekeringskosten per maand te bepalen: hoe veiliger je rijdt hoe minder je betaalt. De automobilist kan hier voor kiezen, nog wel althans, maar in veel andere gevallen is de keus er niet of niet meer. We hebben geen idee wat er precies met onze persoonsgegevens en digitale profielen gebeurt — wie gebruikt ze en waarvoor? Ook is onduidelijk hoeveel geld er omgaat in de data-economie, maar dat het om miljarden gaat is geen geheim. De datastromen onder de motorkap van het internet zijn inmiddels zo ondoorzichtig dat het aan de gemiddelde internetgebruiker ook niet meer eenvoudig uit te leggen is wat er precies gebeurt. Wist u bijvoorbeeld dat wanneer u een website bezoekt data over uw klikgedrag realtime worden geveild? Binnen zes milliseconden is de hoogste bieder bekend en kan deze zijn advertentie plaatsen op een volgende site die u bezoekt. Met de komst van de smartphone is alles zo mogelijk nog minder navolgbaar geworden. Om die reden is het ook lastig, ja zelfs onmogelijk, om als internetgebruiker nog een geïnformeerde keuze te kunnen maken over het gebruik van onze persoonsgegevens door derden. En eerlijk is eerlijk, die keuze hebben we in feite ook al helemaal niet meer.

De in essentie goedbedoelde, maar in zijn uitwerking onfortuinlijk uitgepakte Cookiewet was of is daarvan een zichtbaar bewijs. Cookies zijn kleine tekstbestandjes die websites op computers zetten om onze keuzes en voorkeuren vast te leggen. Sinds inwerkingtreding van de Cookiewet moeten bedrijven en organisaties ons over het gebruik daarvan informeren. Zonder via irritante pop-ups in te stemmen met het gebruik van cookies kunnen we sommige websites nu ineens niet meer binnentreden. Online actief zijn zonder cookies lijkt echter — met of zonder Cookiewet — überhaupt geen optie meer te zijn, ondanks allerlei software die de internetgebruiker op zijn of haar computer kan installeren om de zogeheten 'trackers' — oftewel de bedrijven achter veel cookies die zoveel mogelijk over ons te weten willen komen — te weren. De Amerikaanse onderzoeksjournaliste Julie Angwin doet in haar recente boek 'Dragnet Nation' verslag van haar pogingen om uit te komen onder de door bedrijven en overheden strategisch uitgegooide elektronische sleepnetten die onze persoonsgegevens in grote hoeveelheden en voor uiteenlopende doeleinden digitaal bijeenschrapen. Haar conclusie is dat dit met zeer veel moeite maar in heel beperkte mate lukt. Als experiment zijn haar pogingen weliswaar buitengewoon interessant maar voor het alledaags internetgebruik van de gewone burger veel te omslachtig, veel te ingewikkeld en derhalve geen optie.

Zoals ik zo-even al aanstipte, monitoren niet alleen bedrijven ons internetgedrag, maar doen ook overheden dit en steeds vaker in al dan niet juridisch afgedwongen samenwerking met de private sector die op haar beurt ook in toenemende mate gebruik maakt van door de overheid verzamelde data. Er ontstaat met andere woorden een onontwarbare en ondoorzichtige kluwen aan datastromen in en tussen de publieke en private sector. Het meest aansprekende voorbeeld zijn natuurlijk de recente onthullingen in de media op basis van de door Edward Snowden verzamelde bestanden in de tijd dat hij werkzaam was als systeembeheerder voor de Amerikaanse veiligheidsdienst NSA. De revelaties kwamen voor velen weliswaar niet als een complete verrassing maar de schok over de omvang en indringendheid van de spionagepraktijken was groot en het falen van juridische waarborgen die juist ook onschuldige burgers moeten beschermen is buitengewoon zorgwekkend. Bovendien kunnen er vraagtekens worden gezet bij de effectiviteit van dit soort praktijken. De Amerikaanse onderzoekers Jeff Jonas en Jim Harper concluderen in hun onderzoek dat het niet mogelijk is om op basis van grote hoeveelheden data zeer zelden voorkomende gebeurtenissen, zoals terroristische aanvallen, te voorspellen, te meer deze vaak per geval ook nog worden gekenmerkt door bijzondere omstandigheden. De NSA heeft nog niet overtuigend kunnen aantonen dat zij terroristen ook daadwerkelijk heeft weten te stoppen met haar controversiële sleepnetpraktijken en ook Obama gaf schoorvoetend toe dat terroristische aanvallen die zijn verijdeld wellicht ook heel goed met andere —lees: conventionele — opsporingsmethoden hadden kunnen worden voorkomen. Bovendien glippen terroristen die wel op de

radar van de inlichtingendiensten hadden moeten oplichten door de mazen van het sleepnet heen. Denk aan de ‘Underwear Bomber' die in het vliegtuig onderweg naar Detroit een in zijn onderbroek verstopt — vandaar de naam — explosief tot ontploffing probeerde te brengen en werd overmeesterd door zijn Nederlandse medepassagier Jasper Schuringa. De vader van de terrorist had de autoriteiten al gewaarschuwd dat zijn zoon aan het radicaliseren was. En ook de Fort Hood Shooter die in 2009 onder de in het Arabische geuite uitroep ‘God is groot’ het vuur opende in een Amerikaanse kazerne, waarbij 13 personen werden gedood en meer dan 30 gewond raakten, als ook de Boston Bombers die vorig jaar — u hebt de beelden vast nog voor ogen — een aanslag pleegden tijdens de jaarlijkse marathon in Boston waarbij honderden mensen gewond raakten en drie personen omkwamen. In beide gevallen waren de aanvallers bij de Amerikaanse autoriteiten bekend als potentiële terroristen of op zijn minst als personen die extra aandacht behoefden. Om onze vrijheid te beschermen tegen terrorisme leveren we paradoxaal genoeg veel van onze vrijheid in, terwijl het dus maar zeer de vraag is of deze totale controle terroristen tegen kan houden.

Dames en heren, sinds haar begindagen is het internet zéér ingrijpend veranderd. Het motto van onze universiteit — libertatis praesidium ofwel bolwerk van vrijheid — had aan de poorten van het internet in de jaren 90 van de vorige eeuw zeker niet misstaan. Het internet — of beter gezegd cyberspace zoals de virtuele wereld van computers onder ingewijden bekend stond — werd beschouwd als een plek die losstond van de offline wereld, waar nieuwe virtuele gemeenschappen ontstonden, waar mensen de vrijheid genoten om hun identiteit opnieuw uit te vinden en die — en dat met name was voor ons juristen interessant — niet direct werd bestuurd door een centrale overheid. In feite werd deze omgeving beschouwd als een afzonderlijke ruimte vrij van het bestaande positieve recht, zoals wij juristen het veelal bestuderen, met haar eigen regels, zoals de welbekende netiquette. Op het internet bestaan nog steeds virtuele ruimtes, zoals online games als World of Warcraft of virtuele werelden als Second Life — ja het bestaat nog steeds — die specifieke regels in hun gebruiksvoorwaarden opleggen aan hun inwoners en zelfs een heel eigen virtuele economie kennen. De algemene opvatting vandaag de dag is evenwel dat het recht zoals dat offline geldt ook op ons online handelen van toepassing is. Een overeenkomst tot het kopen van een paar schoenen bij Zalando is net zo geldig als wanneer we nieuwe laarzen bij Invito in de Haarlemmerstraat kopen. Op Marktplaats mag je net zomin iemand oplichten als op de Leidse zaterdagmarkt. En evenals huisvredebreuk is computervredebreuk een strafbaar feit. Internetrecht is daarmee steeds meer een vanzelfsprekend onderdeel geworden van de klassieke rechtsgebieden, zoals het privaatrecht, het strafrecht en het bestuursrecht. Ook al is het techno-sociale en daarmee juridische landschap inmiddels echter flink veranderd, velen van ons zullen het internet desondanks ook nog steeds wel met een groot gevoel van vrijheid associëren. Dat gevoel vindt gelukkig immer nog weerklank

in het recht, maar vanzelfsprekend is het niet en er een ligt een belangrijke taak voor ons juristen om deze te bewaken. Ook kom daar zo graag nog even op terug.

Ondanks het tamelijk sombere beeld dat ik eerder schetste, wil ik u wel verklappen dat ik — ondanks alles — dol ben op elektronische gadgets en enorm enthousiast over de werelden die het internet voor ons opent — informatief, sociaal en ja ook commercieel. Online winkelen is een zegen als je een drukke baan en een hectisch privéleven hebt. Maar was de vrijheid op het internet van de midden jaren '90 van de vorige eeuw werkelijkheid heden ten dage is deze — ook al zijn we ons of is niet iedereen zich daarvan even bewust — steeds meer een illusie aan het worden. Aan alle kanten wordt er aan onze rechten en vrijheden geknabbeld. Nu wij zelf het product worden als we op internet surfen en de overheid steeds ongeremder kan en soms zelfs mag meekijken met ons digitale leven kan dat ten koste gaan van ons vertrouwen in internetbedrijven, de overheid en ook in de technologie zelf. Persoonlijk merk ik dat ik mijn aanvankelijke onbevangenheid op sociale media, als Facebook en Twitter, is verdwenen en ik vraag me serieus af of ik deze accounts niet gewoon helemaal moet opdoeken. Ook neem ik meer en meer mijn toevlucht tot privacy-vriendelijke software, zoals TOR, de browser waarmee je anoniem kunt surfen. En dat is vast heel verstandig als je voor het facultaire openingscollege informatie zoekt over terroristen. Heb ik alle webcams bij ons thuis afgeplakt, zodat geen van onze gezinsleden heimelijk kan worden bespied door 'creeps' en criminele bendes die mijn kinderen naakt dansend in hun slaapkamer — om maar even een hypothetische situatie te schetsen — willen afpersen. Bovendien ben ik vaker bereid om voor beveiligde diensten te betalen. Zo heb ik een mailaccount in Duitsland — het land met de strengste privacywetgeving dat deze ook nog eens serieus handhaaft — en gebruik ik een beveiligde verbinding waarmee je via onbeveiligde WIFI-hotspots — die ons hier overal omgeven — toch veilig online kunt zijn — met andere woorden: zonder ongewenste en wellicht kwaadwillende insluipers in je computer. Want we worden natuurlijk niet alleen door bedrijven en de overheid bespied, maar dat is stof voor weer een ander college. Aan mijn studenten laat ik door middel van visualisaties letterlijk zien hoe met elke klik het aantal commerciële partijen dat hen volgt exponentieel toeneemt en er een web van connecties ontstaat tussen al deze partijen uitmondend in een omvattend beeld van hun persoon. Daarmee krijg je een collegezaal wel even stil, kan ik u zeggen. De eerste vraag is dan steevast: wat kan ik hier tegen doen?

Maar kunnen we de controle terugkrijgen? De spanning tussen geld verdienen — véél, héél véél geld verdienen — en het waarborgen van onze privacy — een toch wat ongrijpbaar concept — is té groot om dat zonder ingrijpen van de wetgever te

realiseren. Een complicerende factor is daarbij dat de overheid zelf belang heeft bij sleepnetpraktijken. Het Hof Den Bosch drukte er afgelopen maand zelfs een stempel van goedkeuring op. De persoonsgegevens van álle klanten die via het bedrijf SMSparking met hun mobiele telefoon parkeergeld betalen, moeten aan de Belastingdienst worden doorgegeven zodat deze belastingfraude kan opsporen. Voor de mensen in de zaal die nu verheugd constateren dat ze een andere mobiele parkeerdienst gebruiken: deze hadden al zonder morren uw gegevens aan de belastingdienst gegeven. Het Hof draait de uitspraak van de voorzieningenrechter in eerste aanleg terug die nu juist onomwonden had geoordeeld dat — en ik citeer — “het dagelijks doen en laten van de burgers […] de overheid niets aan [gaat]”.

Gelukkig zijn er vergevorderde wetgevingsplannen van de Europese wetgever die het datagraaien aan banden moeten leggen. Of dat lukt is een tweede, maar er zijn enkele lichtpuntjes. De meest hoopvolle koers — naast torenhoge boetes voor het omzeilen van de nieuwe regels — is de verplichting voor bedrijven om privacyregels in te bouwen in hun diensten — ‘privacy by design’ noemen we dat. Innovatie en privacy gaan als het ware hand in hand. Een interessant voorbeeld is het door NSA-medewerker Bill Binney ontworpen ThinThread: een sleepnet voor de Amerikaanse veiligheidsdienst waarmee inlichtingen konden worden ingewonnen terwijl de privacy van het individu beschermd bleef. Het systeem kon grote hoeveelheden data binnenhalen die werden versleuteld en slechts dan ontsleuteld en geanalyseerd als zich een specifieke dreiging voordeed. Het moge duidelijk zijn dat het project is gesneuveld en Bill Binney werd zelfs ontslagen. Het zal overigens niet eenvoudig zijn om een complex begrip als privacy en onze sterk uiteenlopende wensen, behoeften en eigenaardigheden dat het omvat te vangen in een technologisch ontwerp, maar deels zouden we die zelf kunnen vormgeven als de zwarte doos met datastromen wordt opengebroken en we zelf aan de knoppen kunnen draaien. Dat is echter niet de enige maatregel. Daarnaast wil de Europese wetgever het geautomatiseerd opstellen van digitale profielen over ons verbieden, tenzij we er zelf mee instemmen. Een goedbedoelde intentie die — evenals de Cookiewet — waarschijnlijk leidt tot gedachteloos doorklikken. We weten tenslotte al langer dat privacyvoorwaarden om allerlei begrijpelijke redenen — te lang, te ingewikkeld, geen tijd — doorgaans niet worden gelezen en bovendien is het opnieuw de vraag of we oprecht een keus hebben. Ook veronderstelt instemming een zekere rationele kennis die haaks staat op de vaak onbewuste en onbevattelijke manier waarop we online worden gemanipuleerd. We zijn niet alleen het product, maar — zonder dat we daar vooraf over geïnformeerd worden — ook het proefkonijn. Zo experimenteert datingsite OKCupid met het koppelen van personen die niet met elkaar ‘matchen’ om te kijken wat er gebeurt en ‘tweakt’ Facebook onze gemoedstoestand door de nieuwsfeed te vullen met negatieve óf juist positieve berichten.

Dames en heren, rond de jaren ’60 van de vorige eeuw begon de digitale revolutie die — evenals de agrarische en industriële revolutie voordien — grote veranderingen met zich bracht en brengt. In onze zich rap en substantieel transformerende samenleving is het essentieel dat de focus mede gericht is op de bescherming van onze fundamentele rechten en vrijheden. De digitale revolutie daagt het recht uit gelijke tred te houden en dat is waarlijk geen eenvoudige opgave gebleken. Het recht op haar beurt omvat echter eeuwenoude waarden, beginselen en rechten die niet in steen gehouwen zijn maar in deze technologisch en anderszins roerige tijden nog steeds van wezenlijk belang zijn voor een menswaardig bestaan. Vanaf deze week zal onze faculteit van start gaan met de internationale master ‘Law and Digital Technologies’, waarin we studenten met zeer actuele, fundamentele juridische vraagstukken op het terrein van digitale technologieën en het internet confronteren vanuit het perspectief van de rechtstaat en fundamentele rechten en hen zullen bekwamen in de academische en professionele vaardigheden om deze vraagstukken met kennis van zaken zelfverzekerd tegemoet te treden. Want het moge u duidelijk zijn geworden, de onderwerpen in dit college, maar — zo kan ik u verzekeren — ook tal van andere onderwerpen op ons vakgebied vragen om een zeer gespecialiseerde academische opleiding.

Tot slot keren we nog even terug naar onze Canadese collega’s in Toronto die op een wel heel wonderbaarlijke wijze werden uitgedaagd nadat ze hun opmerkelijke onderzoek hadden afgerond. Allereerst werden ze geconfronteerd met de vraag hoe om te gaan met de geheime, politiek zeer gevoelige informatie van de Indiase overheid waar ze toegang toe hadden gekregen. Na uitgebreide beraadslagingen besloten de Canadezen om open kaart te spelen, zodat de Indiase overheid digitale gaten kon dichten en nieuwe cyberaanvallen voorkomen. Het contact resulteerde echter in een wel heel curieus — ofschoon niet geheel onbegrijpelijk — verzoek van de Indiase overheid: willen jullie de Chinezen voor ons terughacken? Het antwoord op die tweede vraag was een stuk eenvoudiger en ik hoef u vast niet te vertellen hoe dat luidde.

Dames en heren, rest mij slechts u allen een zeer inspirerend, leerzaam en plezierig nieuw facultair jaar toe te wensen!