Cyberspace: op weg naar de nieuwe rechtvaardigheid of juist totale willekeur

Cliprecht, clickrecht, klikrecht, kliprecht, streamrecht

De ontwikkelingen van Cyberspace, binnen en buiten de orde, werpen vragen op over wettigheid, recht en rechtvaardigheid binnen wat nu onze nieuwe (virtuele) leefruinte is. Zowel het oprukken van de grote portals, het afluisteren door overheden als het hele malware fenomeen en de copyrights op content en software werpen nieuwe vragen op. Kan dit wel, kan dit niet, waar liggen de grenzen? Winnen de hackers, is het hele systeem en de samenleving daarmee kwetsbaar voor totale chaos, en moeten we daarom maar toestaan dat de anti-terreur oorlog hackers en scheefdenkers als de vijand gaat zien? We schrikken af en toe van berichten over massief afluisteren van alles, over gaten in de beveiliging en hoe men door profiling steeds meer over je weet, maar juridisch blijft het een grote gatenkaas, waar men dan wel op nationaal niveau iets aan doet en uitwassen als kinderporno probeert te beteugelen, maar internationaal en juridisch is Cyberspace nog steeds het wilde digitale westen. Ondanks breed gedragen inzichten als netneutraliteit en J.P. Barlow's Cyberspace Independence Declaration doen commercie en regeringen min of meer wat ze willen, censureren en monitoren maar raak. Het graaien in data die om heel andere redenen verzameld zijn, zoals historische gebruiksdata, medische data, privacy gevoelige data, DNA-gegevens neemt in het kader van Big Data een grote vlucht, de enkele successen worden aangevoerd als verontschuldiging voor de praktijken om uit grote bestanden discriminerende particuliere trends af te leiden. Big Data kan gezien worden als gelegaliseerde phishing, en bedrijven als Google praten al over een 'recht op weten' en daarmee criminalisering van privacy.

Recht, wet en ethiek

Er is duidelijk behoefte aan een herijking van ons rechtsdenken betreffende privacy, kennis, intellectuele prestaties, lange termijn implicaties van techniek en de ethiek van de identiteit. Het gedachtengoed van Plato, Aristoteles, Justinianus, Descartes, Spinosa en Grotius voldoet niet meer, de cyberspace dimensie en de technologie van genetische en psychologische determinatie heeft ons menszijn en onze identiteit zo ge-externaliseerd dat het geweten en het categorisch imperatief van Kant niet meer voldoende zijn om vragen over goed en kwaad te kunnen beantwoorden. Er is behoefte aan een nieuw perspectief, dat niet alleen het aloude metafysische (otherworld) denken maar ook de materialistische visie recht doet. Een ecologisch rechtsdenken, zo afwezig in onze christelijk-joods-romeinse traditie (de Tien Geboden missen de ecologische dimensie) is nodig om lange termijn gevolgen van vrijheden en maatregelen 'recht' te doen en stabiliteit op termijn te verzekeren.

Verandering is de basis van het vooruitgangsparadigma, dat is een ander uitgangspunt dan de stabiliteit en handhaving van een onveranderlijke status quo en de daaruit voortvloeiende gedragsregels die de Confucianistische Chinezen als 'Li' formuleerden, en de Aboriginals in hun Ngarra-wet vastlegden en veel meer ecologisch gefundeerd waren dan ons rechtssysteem. Onveranderlijkheid en verantwoordelijkheid voor stabiliteit was daar vanzelfzelfsprekend. In onze tijd, waar we van crisis naar crisis wankelen, de basisparameters qua gezonde leefomgeving en herbruikbare hulpbronnen zijn aangetast, is een nieuwe ecologie nodig, een dynamische ecologie die sturing en begrip voor lange termijn effecten paart aan directe reactie op verstorende effecten. De twee paarden uit Plato's Phaedrus, het wilde creatieve naast het brave conservatieve paard, dienen met beleid gestuurd te worden in het besef dat beiden nodig zijn in de dynamische wereld van de voortdurende verandering.

Cyberspace rechtsvragen

Is het mogelijk om uitgaande van heldere rechtsgronden, met een rationele en dieptepsychologisch verantwoorde maar niet dogmatische basis, voor cyberspace rechtsregels en handhavingmodellen te ontwikkelen? Een moeilijke vraag, want cyberspace, high-tech, globalisering en internet zijn zo verweven, dat een visie op cyberspacerecht eigenlijk niet mogelijk is zonder analyse en duiding van de ontwikkeling van de samenleving in de laatste eeuwen. We zijn op zoek naar rechtsgronden voorbij de geschreven wetten, dat werd wel aangeduid als natuurrecht (Natural Law) maar is grotendeels vervangen door verdragen, geschreven wetten en vastgelegde uitspraken, de jurisprudentie.

Sinds Mozes, Mohammed, Plato en Aristoteles, maar zeker sinds Grotius, Spinoza, Kant, Franklin en Rousseau is de wereld fundamenteel veranderd, zijn onze opvattingen over recht, rechtvaardigheid, waarheid, waardigheid, macht, vertrouwen, vrijheid en zelfs over werkelijkheid gaan verschuiven, maar werken we nog wel met een rechtssysteem dat op z'n best symptomatisch is aangepast aan de nieuwe tijd.

Ik zie daarbij een aantal verschuivingen of zelfs paradigmatransformaties, namelijk de verschuiving in het begrip identiteit, de teloorgang van het integriteitsprincipe (onschuldig tenzij wordt nu, schuldig tenzij) en in het denken over eigendom en dan vooral digitale eigendom.

Wie ben ik? Habeas IP

Het begrip identiteit, wie ben je en waar beroep je je op, is natuurlijk sinds de dagen van de Advaita Vedanta een filosofisch en psychologisch discussiepunt, en we hebben nog steeds geen goed antwoord op vraagstukken als determinisme versus vrije wil, maar het vervagen van de identiteit in cyberspace voegt daar een nieuwe dimensie aan toe. Welke rechter kan een digitale entiteit via een Habeas Corpus opdragen te verschijnen, in persoon. Is je identiteit je IP-nummer, maar dat kan door anderen misbruikt zijn, is het wat je op Facebook zet, op je website, of ook wat je in privé emails en berichten uitwisselt? Gemakshalve wordt dat IP-nummer wel gebruikt om zoals in Duitsland boetes uit te delen bij illegale downlaods, maar de legaliteit daarvan is niet helemaal helder.

Met name op internet, waar we wel IP-adressen of email adress hebben, maar de koppeling naar een persoon of verantwoordelijke steeds moeilijker wordt, is identiteit niet meer gebonden aan een persoon, maar op z'n best aan een dataset. Dat is een berg gegevens waarvan niet eens eenduidig te bepalen is of het om een mens, een avatarconstructie, een (ro)bot, een programma of een "Geest in de machine" dan wel een spontane mutatie van 'artificial intelligence' gaat.

In het bestaande recht is de 'habeas corpus' of het Spaanse 'amparo de libertad' ('bescherming van vrijheid) de klassieke manier om illegale gevangenneming te bestrijden, en bijvoorbeeld vragen over de autoriteit, de 'quo warranto', aan de orde te stellen. Maar hoe kun je een organisatie of bedrijf die aan de haal gaat met je digitale identiteit, je digitaal gevangen houdt, voor de rechter slepen. Er is nu sprake, bijvoorbeeld voor Facebook, van een recht tot vergeten, een recht om je informatie te laten wissen, maar hoe weet je wat men over je weet en heeft opgeslagen. Maar daar stelt Google van haar kant een 'recht om te weten' tegenover, waarmee privacy niet alleen achterhaald, maar bijna tot een criminele zaak gemaakt wordt.

Descartes' adagium 'Cogito, ergo sum' is daarmee onderuit gehaald; zelfs de beperkte zekerheid die de cartesiaanse rationalist veronderstelde, lost op in de digitale brei. Want wat is denken? Neurologen mogen het tegenwoordig zien als 'embodied cognition' en wijzen op de koppeling van ons denken aan zintuigen, maar ' artificial intelligence' rukt op, de denkende machine kan al heel wat dingen beter dan de mens. Alleen het (zelf)-bewustzijn ontbreekt, maar volgens mensen als Ray Kurzweil is dat een kwestie van tijd. Hij ziet de mens opgaan in steeds betere computersystemen, zijn mening is overigens niet onomstreden.

Het vervagen van de fysieke identiteit en sluipend overgaan op een virtuele identiteit is beangstigend en heeft een tegenhanger in de neiging, de materiële identiteit tot op het bot en het DNA van iedereen te willen vastleggen. Iedereen en alles in de computer, de onzekerheid van de echte identiteit proberen te vangen via koppeling van bestanden, profiling, uitvinden wie er achter een email adres, Facebook pagina of website zit. Dat betekent steeds complexere identiteitscontroles, een uitdijende digitale schaduw en aantasting van de privacy. Identiteit en privacy, de onzekerheid over wie wat wanneer en waar is, en wie dat weet of mag weten, wie is te vertrouwen, wie verantwoordelijk, indemniteit; hiermee naderen we een gebied waar de angst bepalend is. Een persoonlijke angst, in hoeverre mag ik denken wat ik wil, streven naar ontplooiing en "individuatie", fouten maken en leren als alles over dat "ik" direct of afgeleid bekend wordt of is? Maar ook een collectieve angst, de gevolgen van hi-tech acties zijn zo overweldigend, platleggen van het internet, betalingsverkeer, biologische en nucleaire fouten of misdaden zo ingrijpend, dat de overheid (of het systeem) daardoor min of meer de vrije hand krijgt en men vrijheid opoffert voor vermeende veiligheid. Het bewust of onbewust opjagen van het angstdenken, leidt, vrees ik, tot steeds meer vervreemding, tot separatie, niet verbinden, eenzaamheid en de compensatie daarvan in virtuele verbanden, social networks en fundamentalisme. De vlucht in onwerkelijkheid, in make-belief, in rollenspel, in extern bepaald en gemanipuleerd consumentisme, in wat Jesse Schell de gameification van de samenleving noemt is onmiskenbaar, je bent wat je voorgeeft te zijn, het masker wordt steeds bepalender, het innerlijke kind of de ziel offeren we op aan het bonussysteem van scholing, carriere, uiterlijke identiteit.

De omkering van het onschuldigheids-aanname en de daaruit volgende veranderingen in opsporingsmethoden, bestandsbeheer en inperking van integriteitsrechten hebben natuurlijk ook te maken met die identiteitscrisis, het gebrek aan vertrouwen en het angstdenken. Gaan we uit van het principe, dat geen onschuldigen mogen lijden om schuldigen aan te pakken, of draaien we het om en is het pakken van een schuldige zo belangrijk dat onschuldige slachtoffers (collateral damage) acceptabel is?

Die keuze is zeer fundamenteel, en we groeien van het eerste model, dat ooit het uitgangspunt was van grondwetten, Bill of Rights en het "verlichte"rechtssysteem, naar met grove middelen; maar in het wild wat schieten, in de hoop een terrorist, crimineel of cyberbedreiging te raken. We zetten het individu letterlijk en figuurlijk in z'n onderbroek, om de pakkans van een enkele terrorist te vergroten. Dat is overigens een tweesnijdend zwaard, zoals Wikileaks aantoonde, want het voedt de overtuiging, dat er ook op het publieke niveau niets verborgen mag blijven. De aantasting van de vertrouwelijkheid is in die zin niet beperkt tot het individu, ook de overheid moet maar aantonen, dat ze onschuldig zijn.

Digitale eigendom, het bezit van zaken, die vrijwel kosteloos vermeerderd kunnen worden, begint steeds verder weg te groeien van oorspronkelijke noties over de materiële en aanraakbare zaken. Hier komt de fundamentele vraag naar boven, wat informatie is en aan welke regels en wetten dat voldoet. In mijn visie is informatie in ieder geval meer dan gegevens, "a bit is only information i fit bytes" maar is het ook meer dan in de unidirectionele visie van Claude Shannon? De klassieke Cybernetica, Cyberspace en de beperkte, maar "bewijsbare" notie dat informatie niet meer is dan een tot verandering leidende uitwisseling van gegevens tussen zender en ontvanger houden geen rekening met een veld-karakter van informatie, met intentionaliteit, met de relatie informatie-bewustzijn-zijn die in de moderne fysica toch steeds evidenter wordt, en in extremo met het magische karakter van informatie. Information wants to be free, de strijdkreet van de cyber-avonturiers en hackers, zit daar een grond van waarheid in, heeft het gekende of te kennen een eigen bestaan, een eigen dimensie, een Akashic entiteit. De relatie tussen informatie en de menselijke geest is in ieder geval complexer dan de aanhangers van de "meat-computer" willen doen geloven, Jaron Lanier (de pionier van virtual reality) z'n wat cryptische uitspraak "Information is alienated experience” legt een duidelijke link tussen informatie en ervaring in menselijke zin. Hij wijst er ook op, dat we onszelf verkopen door deel te nemen aan Facebook etc. en dat we daar eigenlijk voor betaald zouden moeten worden, we zijn dataleveranciers naast gebruikers. In praktische zin zijn er de kwesties van intellectuele eigendom, auteursrecht, innovatie, en weer privacy, digitale schaduw, en de spagaat veiligheid-vrijheid die rond digitale eigendom naar voren komen.

Bij dit alles komt de rol van de overheid, of een overheid danwel op een op contractuele afspraken gebaseerd overkoepeld orgaan, natuurlijk aan de orde.

Is die rol meer dan een het uitvoeren van het “contrat social”, is er een biologische danwel metafysische noodwendigheid of een rationeel imperatief of moeten we denken in termen van een IP-cratie, waar de organisatie met de meeste cyberburgers de moraal bepaalt?

Spinoza zag vrijheid als het taakgebied van de overheid, maar komt dat niet neer op het aangeven van de grenzen tussen het publieke en het private en daarmee van de belangenafweging tussen die twee. Hoe kunnen we in Cyberspace of breder in het hele supernationale recht bereiken dat die grensbepaling en belangenafweging een echte balans is en geen opgelegde dictatuur of anarchistische chaos, van dictatoriale structuren of individuele hackers.

Is het geen tijd voor internationale afspraken, het instellen van een Cyberspace autoriteit op bovennationaal niveau, waar we antwoord zoeken op bredere rechtsvragen en kwesties. Maar dan wel een autoriteit die niet aangestuurd wordt door commerciële belangen, nationale interesses of afhankelijk is van particuliere belangen en geldstromen. Eigenlijk zou zo’n Cyberspace Autoriteit democratische gekozen moeten worden, met alle wereldburgers als stemgerechtigden en in een opzet die stem-manipulatie en polarisatie voorkomt.

Op basis van een analyse van historische meningen en rechtvormen en kijkend naar de nu wat gekunstelde pogingen om die principes en de wetten, verdragen en overeenkomsten toepasselijk te verklaren in cyberspace zouden er nieuwe wegen moeten worden aangegeven om tot cyberrecht en virtuele rechtvaardigheidsprincipes te komen. Van daaruit dan die uitwerken tot wetten, regels, gedragsnormen en handhaving daarvan. Daartoe kunnen aanpassingen van het zee- en oorlogsrecht, het gebruik maken van nieuwe vormen van democratische of gebruikerinvloed met behulp van sociale netwerken dienen.

Voorop staat echter het zoeken naar begrip voor de ontwikkeling van identiteit en individuatie, want de vervreemding van het eigene, het externaliseren van de identiteit en het determineren van een verstikkende digitale (biologische, vastliggende) identiteit is de rode draad in de ontwikkeling van de gestuurde realiteit, die we graag als vooruitgang willen zien, maar eigenlijk steeds onmenselijker wordt.

Breder dan het aanraakbare

Cyberspace is meer dan internet, ik neig ertoe het te zien als de wereld van de virtuele informatie en breek daarmee uit de beperking tot internet, computer-technologie en high-tech. Plato, Kant, de idealisten waren bezig met (en deel van) cyberspace in die zin, maar ook de virtuele wereld van een roman heeft cyberspace kanten, en de verbeelding in brede zin is natuurlijk virtueel, en wat te denken van religie, magie en wijsbegeerte? Het woord informatie voegt een kwalificatie toe aan het virtuele, het gaat om data of gegevens die echte verandering bewerkstelligen. Pas als cyberspace in die zin iets veroorzaakt of verandert is er sprake van echte informatie, echte virtual reality, anders is het niet meer dan ruis. Cyberspace beperken tot internet en computers of zelfs uitbreiden tot high tech helpt niet om de wortels van de problematiek bloot te leggen. Dat zien we bij de aanpak van wat men cybercrime noemt, als we daar de gevaren van nano-technologie, DNA-manipulatie, biologische oorlogvoering etc. bij halen en gaan denken in termen van high tech criminaliteit dan zien we al snel veel bomen, maar herkennen geen bos meer.

Richting

De richting waarin de ethiek en rechtsstelsel voor cyberspace zou moeten gaan, draait dus vooral om identiteit en indemniteit, verantwoordelijk zijn voor wat je aanricht. Via deze navolgende analyse kom ik uiteindelijk bij het besef, dat een nieuwe democratie, in de zin van participatie van betrokkenen, inclusief gebruikers bij regelgeving en de discussie over normen en waarden betrokken moet worden. Dat kan bij gebrek aan bovennationale autoriteiten alleen maar gaan via ICANN en nationale wetgeving, waarin de verplichting tot in eerste instantie consultatie van gebruikers en klanten kan worden opgenomen. Daarbij zullen nieuwe rechten en plichten moeten worden betrokken, zoals click- en cliprecht.

Rechten- en plichtenloze jungle in cyberspace.

Al in 1996 stelde een rapport van de Nederlandse Vereniging van Informatietechnologie en Recht; ‘Regels kent de virtuele wereld niet, althans nog niet’. Anno 2011 zijn we nog niet veel verder, is er wat gebeurd op het gebied van privacy, en juristen worden rijk aan het formuleren van cyber-contracten, maar is het verder een wat gekunstelde situatie, die bovennationaal en nationaal niet duidelijk is en waar gesteggel op bovennationaal niveau nog weinig concreets heeft opgeleverd, terwijl meer helderheid over wat mag en niet mag in cyberspace hard nodig is. Wikileaks en Snowden’s onthullingen over de NSA maakte dat erg duidelijk, en het wat onterecht afgekraakte Faber-rapport (413 pagina’s uit 2010) geeft in ieder geval inzicht en overzicht in wat er fout kan gaan en fout gaat in een beperkt aantal domeinen/clusters van de cybercriminaliteit en hoe profiling in die context gebruikt kan worden.

Cyberspace is geen juridisch terra incognita, zo laat de jurisprudentie zien, men probeert en slaagt er ook vaak in bestaande wetten zo te interpreteren dat ze ook op virtuele situaties van toepassing zijn. Maar er zijn veel grijze gebieden en dan zien we dat waar controle op en handhaving van rechtsnormen ontbreken of falen, het recht van de sterkste of, de slimste of de brutaalste, prevaleert.. Er is geen echte moraal in Cyberspace, en geen heldere ethiek, want natuurrecht of geopenbaarde wetten zijn er (nog) niet in de virtuele wereld. Er zijn wat wetten uit de harde wereld die min of meer van toepassing zijn verklaard, maar een heldere ethische of juridische visie op deze wereld die “wijn verkoopt zonder flessen” zoals JP Barlow (EFF) stelde in 1994, is er niet. Er is nogal wat te doen rond de gebruik en misbruik van content, malware, privacy en veiligheid, de Wikileaks affaire (eind 2010) is maar een recent voorbeeld. Het gaat om muziek, video, maar ook zogenaamde geheime communicatie en dat is niet alleen een kwestie van privacy, openbaarheid van bestuur, criminaliteits-bestrijding, kindermisbruik, terrorisme, nationale veiligheid, maar daaronder zit de kwestie van wie bezit wat aan informatie en wat mag en kan daarmee gebeuren. Dat speelt dan in een wereld, waarin door digitalisatie en globalisering transparantie van alle verkeer, alle persoonlijke data, alle voorkennis en op den duur zelfs je gedachten en emoties (via gelaatsherkenning en emotiesignalering van camerabeelden) openbaar of in ieder geval toegankelijk worden, voor de overheid, commercie en kwaadwillenden die weten hoe ze daar bij kunnen komen. Dat laat een dermate gerichte "profiling" toe, dat de individuele vrijheid zodanig beperkt kan en zal worden, dat psychologische en uiteindelijk somatische schade voor individuen en gemeenschappen dreigt. Gekoppeld aan biometrische data, DNA, vingerafdrukken, irisscans, potentieel allemaal vol privacygevoelige gegevens, ligt een groot deel van je 'objectieve' statistische profiel al zo vast, dat artsen, verzekeraars en overheid er acties op kunnen baseren.

Er is een tendens om door bestandskoppeling en filtering te komen tot zodanige "profiling"van potentiële cybercriminelen dat die preventief diepgaander kunnen worden aangepakt en in de praktijk gestigmatiseerd, waarbij het in de aanvang genoemde risico van aantasting of erger van de rechten van onschuldigen voor lief wordt genomen. De in dat zeer uitgebreide Faber rapport, dat een breed overzicht geeft van de profiling die met alfanumerieke data mogelijk is, genoemde methodes zijn echter nog kinderspel vergeleken met de op video- en beeldmateriaal gebaseerde profiling en risicoprofielen zoals b.v. TNO die onderzoekt en ontwikkelt, of met de stemanalyse, brainscans, MRI of zelfs DNA-analyse die in ontwikkeling is. Een eenvoudige speekseltest wordt al ingezet om commercieel potentieel mee te bepalen, naast psychologische tests. We stevenen daarmee af op technieken, die doen denken aan wat in de tijd der heksenvervolging gebruikelijk was, je bent schuldig totdat je bewijst het niet te zijn, en daarvoor krijg je niet de ruimte of rechtsmiddelen. De praktijk van "Rendition" door de Amerikaanse CIA met instemming en medewerking van vele, ook zogenaamde beschaafde landen, bewijst dat een dergelijke rechteloze vervolging geen illusie is. Waar veiligheid bij terrorisme-bestrijding al voldoende rechtvaardiging is om mensen in hun onderbroek te zetten, zijn de dreigingen van cybercriminaliteit of cyberwar zodanig, dat men nog veel verder zal willen gaan, niets blijft verborgen, en via discriminatie belanden we dan bij specificatie, en gaan we ongetwijfeld preventief toeslaan, met zoveel collateral damage, dat steeds meer verzet dit tot een guerilla-oorlog gaat maken en we allemaal verliezen.

Rechtsvraag

De voorliggende en steeds actuelere vraag is; vereist Internet herziening van het bestaande recht en wet apparaat of biedt het huidige rechtskader voldoende flexibiliteit om ook in cyberspace in redelijkheid normen en waarden te handhaven?

Het is voor velen, maar niet voor iedereen duidelijk, maar men kan de bestaande wet- en regelgeving niet zonder meer op de online-wereld van toepassing verklaren. De digitale identiteit en de rechten daarvan of daarop schept een nieuwe persoonsvorm, een rechtspersoon voorbij de fysieke identiteit, maar wel een die kan handelen, aansprakelijk gesteld kan worden, vrije wil kan worden toegedicht.

Voor (delen van) cyberspace kan of moet dus een ander, bijzonder rechtsregiem gelden, en dat is voorlopig een kwestie van consensus en afspraken, die soms tussen staten, maar meestal tussen wereldwijd actieve partijen op contractbasis gemaakt moeten worden. Voorwaarde is dan wel dat iedere gebruiker en iedere aanbieder van informatie op het net daarmee instemt, al dan niet door zich via een IP-adres, website of via een provider contractueel te verbinden of in te stemmen met aansluitingsvoorwaarden. Dat betekent dat er heldere contractuele regels geformuleerd moeten worden, waar alle partijen zich aan dienen te conformeren, maar daar komen dan nationale en culturele verschillen in beeld, wat voor de een acceptabel is, hoeft dat niet voor de ander te zijn, denk maar aan de censuur die bepaalde landen uitoefenen, al dan niet om politieke of religieuze redenen.

Maar naast rechten, naast transparante en net-neutrale toegang en vrijheid van meningsuiting heeft de gebruiker ook plichten. Als die contractueel zijn overeengekomen kan daar duidelijkheid over bestaan, maar hoe staat het met de digitale burgerrechten en de daar bij horende verplichting om zich ook in een online-omgeving conform de maatschappelijke zorgvuldigheid te gedragen, het ontbreken van een machtsevenwicht is daar duidelijk.

Entropie

Die trend kan ook gezien worden als een entropische tendens, vervlakking en vergrijzing van alle content, de VR-pionier en digitale filosoof Jaron Lanier beschreef de Wikipedia trend en de grootste gemene deler aanpak daarvan al eens als Digitaal Maoïsme, de macht van de middelmaat. We denken dat er meer informatie als in negentropy (dus ingaand tegen de vervlakking) is, en dat lijkt op te gaan voor individuen en bepaalde niches, maar over het geheel genomen glijden we af naar niksigheid, en dat heeft enorme gevolgen. Kijk maar naar de economie, winst is vaak een gevolg van informatieverschil, valt dat weg doordat iedereen alles kan weten, dan verdampt die kenniswinst, en wordt winstopslag een utility-proces op basis van financiering, logistiek, beschikbaarheid etc. Arbitrage, ooit een specialisme van bankers, is nu haalbaar voor iedereen met een internet-aansluiting. Ook voor veel beroepen, die het moeten hebben van gespecialiseerde kennis, is op den duur het internet hun bankroet, want wie heeft hun kennis nodig als het zo te googlen is? We zijn er nog niet, en dus hebben accountants, notarissen, verzekeraars, banken en de pers nog een functie in filteren, verwerken en toegang bieden, maar op den duur worden die domeinen veel minder winstgevend. Ook voor de medische wereld, waar nu al transparantie de zwakke ziekenhuizen en slechte doktoren in hun hemd zet, gaan we die kant op.

Totale transparantie, het duurt nog even, maar hebben we er wel een juridisch fundament voor, zijn onze wetten en ons rechtsdenken wel bestand tegen Wikileaks, peer-sharing, downloads van van alles en nog wat? Vrijheid, veiligheid, privacy welke dimensies van ons bestaan zijn hier in het geding, welke afwegingen bepalen het recht, daar waar de wet ons in de steek laat. Het gaat niet om harde en rationele overwegingen, je kunt bijvoorbeeld niet stellen dat openbaarheid van bestuur altijd prevaleert of dat privacy aantasting uiteindelijk leidt to hogere kosten voor psychische gezondheidszorg, het zijn allemaal vragen die E. Kant in de sfeer van het “Vernunft” plaatste, het domein van de redelijkheid, van de ethiek en daarmee het metafysisiche, want wat is goed en kwaad, zeker als we niet weten wat de uiteindelijke gevolgen zijn van zoiets als Wikileaks of in bredere zin totale transparantie van alle communicatie.

Cyberspace rechtsgronden

Ik denk dat we een ander rechtsparadigma moeten ontwikkelen, een rechtssysteem voor cyberspace, iets als wat Hugo de Groot opzette voor het zeerecht op de vrije zee, maar dan zonder de totale vrijheid en feitelijke wetteloosheid die hij daarmee schiep. Daarbij moet een goed begrip van transparantie, de implicaties en de effecten daarvan op termijn worden bestudeerd, want daar is nog weinig begrip van en voor. Denk maar eens aan wat in het Nederlands dan heel toepasselijk Klik-recht zou kunnen heten. Klokkenluiders, Wikileaks, maar de overheid werkt ook steeds meer met kliklijnen. Wie heeft een klikrecht, wat zijn de ethische bezwaren en voordelen, moeten we terug naar Spinoza om te begrijpen wat ethiek en vrijheid, want daar gaat het uiteindelijk om, hier mee te maken hebben.

Recht en wet waren in het Wilde Westen zeg maar in ontwikkeling, oude stamgebruiken en eigendomsconstructies kwamen er in contact met een Angelsaksisch en deels Latijns rechtsbeginsel dat ook nog tamelijk persoonlijk werd geïnterpreteerd door vrederechters en revolverhelden. Nu is cyberspace de nieuwe grensstreek, waar recht en wet nog vorm moeten krijgen. Volgens sommigen zijn de oude Latijns-Rijnlandse uitgangspunten en de Berner conventie genoeg om ook cyberspace en internet aan te kunnen, maar ik denk dat we wat verder moeten gaan, niet alleen qua wetten en bovennationale regelingen, maar ook qua inzicht in wat rechtvaardig, gewenst en “goed”of “slecht”is. De moraliteit van cyberspace dient naast het zgn. contractsdenken ook een ethische basis te krijgen, de zaken alleen regelen op basis van onderlinge en niet-democratisch opgelegde regelingen en verdragen is onvoldoende en zal uiteindelijk leiden tot revolte en hackerheroïsme. Misschien moeten de Tien Geboden maar uitbreiden met een paar Cybergeboden of moet het eerste Gebod wat worden aangepast tot: “Gij zult de netneutraliteit eerbiedigen”. En kunnen we Kant’s categorisch imperatief als de (niet extern opgelegde of dogmatische) leidraad van het zedelijk bewustzijn “ je moet handelen op de manier waarvan je zou willen dat iedereen zo zou handelen” voor cyberspace interpreteren?

Cyberspace is nieuwe, voorlopig onbegrensd en biedt enorme economische mogelijkheden, maar mist een duidelijke moraal en regelgeving. Al snel wordt daarom de link gelegd naar het Wilde Westen maar ook naar Hugo de Groot, die in 1609 met zijn boek “Mare Liberum” of Vrije zee de grondslag legde voor het zeerecht. Hij poneerde dat de zee vrij was, dat geen enkele natie daar meer rechten had dan andere en dat iedereen gebaat was bij vrije handel en visrechten en dat het een algemeen goed was om de zeeën vrij voor iedereen te houden; het was voor alle landen een nadeel als de zeeën eigendom van bepaalde landen waren. Die visie is, hier en daar wat aangepast zoals wat betreft de zeggenschap over kustwateren, nog steeds de basis van het zeerecht, maar ondertussen is ook wel duidelijk dat daarmee wel rechten, maar geen plichten ontstaan. In zijn tijd was het al een pleidooi voor onbeperkt plunderen en vechten op zee, want het was bedoeld om de zeggenschap van Spanje en Portugal op de Indieroute te ondermijnen, maar tegenwoordig illustreert de deplorabele toestand qua milieu en visstand dat Mare Liberum geen echt verstandige aanpak is. Zonder meer dezelfde principes toepassen op Cyberspace is dan ook onverstandig.

Spinoza

Beter kunnen we kijken naar wat Spinoza dacht over vrijheid, want vrijheid is de taak van de staat of de politiek. Hij ging niet uit van een tweedeling tussen natuur en bovennatuur, en de verordeningen Gods van de religies waren voor hem geen morele principes die ons van boven worden aangereikt, maar principes die berusten op inzicht in het wetmatige karakter van de natuur en de eigen plaats die men in het geheel van de natuur inneemt. Morele waarden vloeien voort uit inzicht in wat goed is voor het individuele en maatschappelijke menselijke welzijn. Hij zag de volbewuste rede wel als een ideaal, maar accepteerde dat die wezenlijk en blijvend verankerd is en verbonden met onze affecten/aandoeningen, onze emoties. We zijn daarom niet redelijk, we kunnen het met moeite hoogstens enigermate worden. Daaruit volgt, dat wetten er van uit moeten gaan, dat er controle nodig is, en er dus goed moet worden nagedacht over mogelijk misbruik door “nog niet redelijke” burgers en gezagsdragers, er moeten checks&balances zijn.

Natuurlijk is er de laatste decennia wel gedacht over de noodzaak van wetgeving, regulering of een supranationale cyberpolitie, maar men hield het vooral op zelfregulering, de Amerikaanse regering hield met name vast aan een “hands off” filosofie, tamelijk libertijns, want men geloofde dat te veel overheidsbemoeiienis de innovatie en economische en technische ontwikkeling zou schaden. Er kwamen wel verklaringen en vage afspraken, de Bonn Declaration uit 1997 is een voorbeeld, maar echte regelgeving en handhavingsinstanties kwamen er niet, buiten de contractuele afspraken die werden gemaakt door de technische partners, providers en de IP-autoriteit (ICANN). In de technische specificaties zoals IPv6 zit wel een zekere dwang, in feite bepalen standaardisatie-organen vaak de richting van de ontwikkeling en kunnen bepaalde ontwikkelingsrichtingen afsluiten, maar dat is beperkt.

SF en ethiek

De huidige ontwikkeling van de techniek en met name cyberspace is voorzien en in zekere zin voortgebracht door de Science Fiction schrijvers, Gibson is een goed voorbeeld, hij kwam met de term Cyberspace. De wetten van de robotica van Isaac Asimov zijn een ander, en treffend voorbeeld, van het bewustzijn bij de SCiFi schrijvers dat ethiek, wetten, wetteloosheid duidelijk aanwezig is en was. 1984, Brave New World, Big Brother, ons denken over Cyberspace is heel vaak gebaseerd op “memes” die in de literatuur naar voren komen.

Klikrecht

Klikrecht, het openbaar willen en kunnen maken van informatie die verborgen werd gehouden, is zo’n onderwerp, waar de rechtsgeleerden zich eens over zouden moeten buigen. Het gereedschap van de huidige rechter, die hier particuliere en publieke belangen moet afwegen, is beperkt, men kan denken in termen van proportionaliteit, maar de tijdsfactor is erg onzeker. Wat is het gevolg van wel of niet naar buiten komen met die gegevens, waren er andere wegen, is een beetje schudden wel en de boom omzagen niet acceptabel. Klikrecht, één van de grote vragen, en niet alleen in cyberspace in 2011!

Het afwijzen van klikken lijkt eenvoudig, in situaties waarin dat ingaat tegen de overheid zoals bij Wikileak roept men om maatregelen, maar het probleem is dat de overheid klikken stimuleert, deals maakt met criminelen over getuigenissen, betaalt voor CD's met bankgegevens, kliklijnen opzet en dan moeilijk kan volhouden, dat voor wat betreft klikken "Quod licet Jovis, non licet bovis" zou opgaan, want waar is dan het rechtsevenwicht. En dat is in cyberspace nu juist de kernkwestie, want daar is geen echte overheid en moet alles dus evenwichtig worden opgetuigd.

Klikrecht in Nederland

Kliklijnen, betalen voor crimineel verworven gegevens, deals met kroongetuigen, aan uitlokking grenzende opsporingsmethoden, het is allemaal vrij gewoon geworden, maar ook vrij eenzijdig gericht op informatie van en door de overheid, inbreuk op grondrechten van burgers zoals het recht op privacy (artikel 10 Grondwet en artikel 8 EVRM) of het weigeren van inzage in processen verbaal is vrij normaal, maar klagen over de overheid wordt extreem moeilijk gemaakt. Er is echter geen specifieke (formeel) wettelijke basis voor klikken ofwel de inlichtingeninwinning door middel van al dan niet anonieme informanten en voor wat betreft klikken over de overheid is dat in de praktijk goed afgeschermd, als men geen betrokkene is kan men bijvoorbeeld over politieoptreden of van ambtelijk misbruik geen aangifte doen en ook de zgn. integriteits-bureau's van de gemeente staan niet open voor klachten die niet gedragen worden door politieke of ambtelijke klagers. En bij klachten is de hele procedure vaak gebaseerd op intern en niet onafhankelijk onderzoek, zonder verdere controle door een onafhanelijke rechter. Voor zover de gedachte wordt aangehangen dat de politie en de overheid al datgene mag doen, wat ook gewone burgers mogen, is een wettelijke regeling voor het passief ontvangen van informatie misschien overbodig en men kan inlichtingeninwinning ook zien als een normale politietaak die, evenals het leggen en onderhouden van contacten met andere burgers, volgt uit artikel 2 Politiewet 1993. Gaat het om inlichtingeninwinning met het oog op de opsporing van strafbare feiten, dan zijn er andere taakstellende artikelen, zoals de artikelen 141 en 142 Sv. Maar voor het het actief runnen van informanten en zelfs betaling voor hun werk, dat vaak een duidelijke aanslag op de privacy van derden inhoudt, is echter geen wettelijke regeling gekregen. Ook in de samenwerking met buitenlandse diensten, in extreme gevallen leidend tot zgn. rendition, gevangenhouding en zelfs marteling, gaat dat ver buiten iedere wettelijke regeling om, en in strijd met het strafvorderlijke systeem in ons land. Situaties waarin de politie informanten strafbare feiten laat plegen en eventueel strafvorderlijke deals met criminelen worden gesloten, zoals de IRT affaire duidelijk maakte, hebben geen wettelijke grondslag. Met betrekking tot het runnen van informanten in de praktijk wel is er de CID-regeling 1995, de (niet-gepubliceerde) Regeling tip-, toon- en voorkoopgelden (1985) en de Modelbrief deals met criminelen (1983), maar die laten veel ruimte, vooral voor korpsen die kunnen afwijken van wat het departement voorschrijft, zoals bleek na Kamervragen hierover. Met name de regel, dat het optreden van de informant binnen de door de rechtspraak gestelde grenzen moet blijven, blijkt niet nageleefd te worden.

Nu is er ook wel iets te zeggen voor betalen voor informatie of zelfs voor het uitloven van premies voor actie. In het Wilde Westen werd het gebrek aan politie en handhaving gecompenseerd oor een systeem van premies en bounty-hunters, dat we allemaal wel kennen uit de Westerns. In cyberspace zou dat een oplossing kunnen zijn en in feite betalen grote platforms als Google en Symantec al voor tips en informatie over gaten in de cyberverdediging, een systeem waarbij klikken over cybercrime wordt beloond is niet ondenkbaar en zelfs het stimuleren van aanvallen op spammers en malware verspreiders is denkbaar..

Normen en waarden en Internetopvoeding

Als we er van uitgaan dat er zekere normen en waarden (moeten) bestaan op internet, dan is alleen repressie onvoldoende om dit op lange termijn te verzekeren, dan zal in de opvoeding aandacht besteed moeten worden aan die regels, normen en ethische waarden. Daarbij komt onvermijdelijk de vraag naar boven, waarom er een scheiding is in de publieke (feitelijk een nationale en een bovennationale) en de particuliere sfeer en waar die ligt en dan komt de privacy weer om de hoek kijken.

Click en Clip

Het gaat ook om rechten, de Wikileaks files zijn eigenlijk copyrights van de betrokkenen,. Auteursrechten en Copyrights, officieel valt dat onder de noemer 'intellectuele eigendom' van digitale media. Volgens de kenners zijn de huidige wetten en regelingen rond het auteursrecht in principe ook bruikbaar voor het digitale en cyberdomein, maar er wordt, met name onder druk vanuit de VS, toch gewerkt aan uitbreiding van met name de Berner verdragteksten en de Universele Auteursrecht Conventie, die de internationale wederzijdse erkenning van intellectuele rechten regelen. Het auteursrecht is een economisch factor, maar ook een culturele, want het is "een motor van de vrije meningsuiting want het verschaft de economische prikkel om gedachten en gevoelens te scheppen en te verbreiden.''

Merken, namen, vormgeving, het valt allemaal onder die intellectuele rechten. Misschien heeft u daar weinig boodschap aan, maar dat kan veranderen. Is uw bedrijfsnaam nog niet door een ander (cyberkraker) als web-domain geregistreerd of gebruikt een of andere grapjas uw prijslijst via een directe verwijslink in zijn pagina als de zijne? Copyrights worden steeds belangrijker, het idee van de 'hackers' dat het om 'onverdedigbare' en dus niet afdwingbare rechten zou gaan is sinds de afgang van de Nederlandse digerati tegenover Scientology (Karin Spaink en consorten verloren dat en terecht, maar verklaarde schaamteloos haar afgang als overwinning, ondertussen won Scientology reeksen zaken over de hele wereld) wel verdwenen. Information wants to be free, een devies waar John Barlow's EFF ooit mee schermde, gaat niet en zeker niet altijd op, tenminste niet in de huidige rechtsorde.

Digitale copyrights zijn lastige dingen, organisaties als Buma/Stemra/Brein gaan er met de techno-fascistische botte bijl achteraan en maken bijvoorbeeld het maken van leuke YouTube filmpjes of websites haast onmogelijk, als er maar een regeltje muziek of songtekst op staat krijg je hen of hun internationale zusterorganisaties en de portal-operators achter je aan. Maar ook de civiele aanspraken van al dan niet vermeend rechthebbenden kunnen uit de hand lopen. Toen we zelf, al jaren geleden overigens, van een of andere louche advocaat een vordering van toen fl 45.700,- kregen omdat een ingezonden brief van een lezer op onze website belandde schrokken we wel even, want inderdaad dat soort zaken is meestal (nog steeds) niet goed geregeld en dus kan iedere gek vragen wat ie wil.

Niet alleen sex

De meeste commotie is op dit moment rond de aansprakelijkheid van site-beheerders en providers voor de veiligheid bedreigende zaken rond terrorisme of nare informatie over wat overheden en bedrijven zoals uithalen (Klik-data).
Overheden blokkeren soms hele reeksen sites, waar kritiek op hun beleid staat, China is een bekend voorbeeld. Maar ook zaken als kinderporno, sex en opruiende, racistische of anderszins onbehoorlijke data, die over landsgrenzen heen verhuizen, halen de kranten. Daar zijn ondertussen voldoende uitspraken over (bv One-to-One versus BT/Ictis en Playboy versus Frena) die duidelijk maken dat er wel degelijk grenzen zijn aan de digitale datavrijheid. Op lange termijn onduidelijker zijn de meer zakelijke rechten, zoals auteursrecht op bestanden met persoonsgegevens, kopierecht, aansprakelijkheid voor de inhoud (smaad), de naamgeving en het merkenrecht, de aansprakelijkheid van de poster, de doorgever en de provider, maar ook de opkomende en nog heel vaag beschreven rechten als click-recht en cliprecht en misschien vanwege de toenemende cloud-technologie ook streamrecht.
Daarbij moet er naar twee kanten gekeken worden, enerzijds de vrijheid van meningsuiting, de rechten en plichten van de eigenaar/opsteller/provider van data en anderzijds de rechten van de burger, bv. de bescherming van z'n persooonlijke levenssfeer en privacy, zoals via de Wet op de persoonregistratie wordt geregeld. De EU heeft hiervoor ook al zgn Data Protection Directives doen uitgaan.

WIPO en ACTA

In Geneve is de WIPO bezig om ook databases als aparte categorie (sui generis) auteursrechtelijk te beschermen, dat zou bijvoorbeeld de ruzies rond telefoonboeken in het voordeel van de PTT's beschermen, maar ook de rechten van de burger op b.v. z'n eigen gegevens drastisch beperken, die komen dan te liggen bij de compilator. Tegen die WIPO plannen bestaat wel verzet, met name vanuit de bibliotheekwereld, die ook het inzagerecht of leesrecht in bibliotheken in gevaar ziet komen
(http://ksgwww.hardvard.edu/llp/datacon.html of
http://www.essential.org/cpt).
Een andere internationale regeling, namelijk het anti-namaak en piraterijverdrag ACTA, dat eigenlijk vooral gaat over namaak van kleding, merkvervalsing en dergelijke, heeft veel discussie opgeroepen, omdat bepaalde passages ook op internet-uitingen zouden slaan. Maar, zei zei minister Van der Hoeven (Economische Zaken) woensdag 8 september 2010 in de Tweede Kamer "er verandert niets voor de internettende consument. Het brengt bijvoorbeeld geen 'three strikes out' aanpak naar Nederland en de vraag of er sprake is van inbreuken op het auteursrecht blijft gewoon een nationale aangelegenheid.".
Het ACTA-verdrag tussen de EU, de VS, Japan en een aantal andere landen is gericht op het maken van betere internationale afspraken om schade door namaak en piraterij te voorkomen. Het gaat om een fenomeen van internationale omvang met grote gevolgen voor veel ondernemers en consumenten die de dupe zijn van namaak en piraterij.
Waar het om gaat is dat door het uitbreiden van de auteursrechten in het digitale domein bijvoorbeeld het browsen of zoeken naar bepaalde informatie afgedekt kan worden. Feitelijk is het al zo dat wat Altavista en Yahoo en zo doen eigenlijk niet mag, je kunt niet zonder voorafgaande toestemming andermans bestanden gaan indexeren en het resultaat aan derden verkopen. Ook het cachen, spiegelen of werken met proxies mag eigenlijk niet zonder voorafgaande toestemming en dat is feitelijk een bom onder het hele idee van kabelmodems etc. Dat wil men beter regelen, maar daarmee gooit men misschien meer overboord dan nodig en rechtvaardig is. Want zonder inzage of zoekrecht wordt ook de mogelijkheid van controle van bepaalde bestanden een wassen neus, want als je ergens niet - zonder betaling - in mag kijken zul je nooit weten of bepaalde gegevens over jezelf, je bedrijf of wat dan ook niet kloppen.
Hoewel met name de uitgevers geporteerd zijn van het idee dat alle digitale bestanden beschermd zijn door een eigen soort auteursrecht is de samenleving daar misschien niet zo bij gebaat. Want controle van bestanden, controle van wat er mee gebeurt is daarmee moeilijk en wekt weerstand, met Wikileak toestanden als gevolg. Wat is digitale en "echte" waarheid in deze zin? Er ontstaat naast de 'echte' burger ook een 'virtueel' beeld van die burger, met b.v. koopgedrag, ziektes, subjectieve beoordelingen, status als consument of kredietwaardigheid, waar men geen weet meer van heeft en waar geen controle op mogelijk is. Het ene land kan proberen zoiets wettelijk te regelen, maar als bepaalde landen niet meedoen gaat het mis. Als b.v. Tonga niet meedoet aan een bovennationale regeling zet men toch de database ergens op een Tonga server (of op een satelliet in naam van Tonga). Of gaat dan een grootmacht of de VN hier oorlog om voeren en Tonga bezetten, ook in het oorlogsrecht zijn we nog niet echt klaar voor cyberspace en cyberwars?

Cyberwar

Cyber-aanvallen op landen (in 2010 Estland) zijn realiteit. Verreweg de meeste specialisten zijn het erover eens dat het bedrijfsleven, maar ook instituties op nationaal en internationaal niveau in de nabije toekomst te maken krijgen met grootschalig cyberterrorisme en/of een grote cyberaanval. Er worden nu door leger en veiligheidsdiensten, de Navo etc. al speciale afdelingen gevormd, het blijkt dat alleen bepaalde interne netwerken binnen de overheid en financiële instellingen relatief goed beveiligd zijn, maar dat is niet dekkend.
De complexe en door cloud technologie nog complexer wordende structuur van informatie- en communicatievoorzieningen is extreem gevoelig voor ontregeling door fysieke aanvallen met e-bommen, DDoS of logische aanvallen met software programma's, ook door vijandelijke staten. Computernetwerken gaan het primaire doel van vijandige machten vormen.

Verschillen in religieuze achtergrond en ethische motieven zijn vaak de aanleiding, dat maakt het allemaal zo moeilijk, want dan ziet men vaak het “opleggen” van Westerse en neoliberale rechtsregels al als een provocatie, en rechtvaardiging van subversieve acties. De filosoof Peter Sloterdijk merkt terecht op ‘Pas op het toppunt van de moderne tijd wordt ons onthuld dat subjectiviteit en bewapening identiek zijn.’

Evenwicht, het Balinese kliprecht

Misschien is het verstandig ons af te vragen wat de onderliggende evenwichten en balancerende krachten zijn of zouden moeten zijn. Wat is de basis van een “klik”-recht (clickright) om te kijken naar bestanden (vergelijkbaar met het inzien van boeken in een bibliotheek) of het clipricht (een soort variant op het kopieerrecht), tot hoever strekt het klikrecht (klokkeluiders) en hoe zit dat met de rechten en plichten van zowel degene die materiaal op het net zet als degene die er naar kijkt. Zouden we bijvoorbeeld geen instantie moeten hebben die wel toegang heeft tot alle bestanden, zelfs die zijn afgeschermd voor het publiek.

Heel vaak vergeten we dat aan wetten ook rechtvaardigheid ten grondslag ligt of zou moeten liggen, dat rechten en plichten met elkaar verweven zijn. De historie kan dat verduisteren en dan komen er soms oorlogen van, met verschrikkelijke tragedies, alleen maar omdat de ene partij zich niet voldoende verdiept heeft in de basis van bepaalde rechten.

Dit zijn rechtsvragen, waar nog eens stevig op gestudeerd moet worden. Daartoe verwijs ik hierbij graag naar wat sommige juristen zich misschien nog herinneren, namelijk het Balinese KLIP-Recht, een soort overgeleverd jutrecht. Een bijna obscuur onderwerp, waar je zelfs op het Internet niets over zult vinden, maar in de vorige eeuw wel de oorzaak van een verschrikkelijke slachting en de teloorgang van een aantal balinese vorstendommen en vorstenhuizen in wat men zich daar nog herinnert als Puputans, bijna rituele zelfmoorden van balinese vorsten en hun familie, die volgens hun eer en geweten het door de Nederlandse overheersers ongeldig verklaarde KLIP-Recht (Tawan Karang) van de onder hen staande bevolking niet wilden (en in hun visie niet mochten) afpakken. Een zwarte bladzijde in onze koloniale geschiedenis, vooral omdat de rechtmatigheid van het verzet van de Balinese vorsten nooit is erkend. Het kliprecht was het excuus voor 5 militaire expedities naar Bali (1846 tot 1906), de ondergang van Badung en Tabanan en de KlungKung puputan van 20 september 1906. Voor de slachter van de Atjeh-oorlog, de toenmalige gouverneur generaal J.B. van Heutz misschien een handige aanleiding om het zelfbestuur van Bali min of meer te beeindigen, voor de Balinezen blijft het onrecht.

De stap van kliprecht naar cliprecht is meer dan een woordspelletjes, het spul dat je toevallig vindt op het strand mocht je volgens dat kliprecht houden, maar de vraag is of er ook geen verplichtingen waren, zoals het brandend houden van lichtsignalen, vuurtorens of betonning. Voor het klikrecht van ons cybertijdperk kunnen we een dergelijke vraag stellen, brengt vrije toegang tot data helemaal geen verplichtingen met zich mee. Misschien moet je betalen, maar je zou ook kunnen denken in termen van een soort burgerplicht om de beheerder van data erop te wijzen, dat er ergens een fout staat. Ik weet het niet, maar dat we de rechtsvragen in cyberspace niet kunnen afdoen met eenzijdige rechten dan plichten kunnen we leren van dat Balinese kliprecht. Checks and Balances, daar draait het om.

Luc Sala