Stichting Digitale
Infrastructuur Nederland

Visie op de relatie Internet en Overheid

DINL - november 2014

Inleiding

Het internet is een technologische innovatie die vrijwel alle aspecten van de samenleving raakt. Als historici over 100 jaar terugkijken op dit tijdperk dan zullen ze een ontwikkeling zien die sterk lijkt op de industriële revolutie. De agrarische samenleving veranderde toen ingrijpend. Handwerk werd vervangen door machines. Dat leidde tot verlies van werk, maar creëerde ook kansen en innovaties die uiteindelijk leidden tot grotere welvaart voor iedereen.

We leven nu in de tijd van de digitale revolutie. Alle informatie wordt digitaal en dit keer is het de informatietechnologie die leidt tot ongekende nieuwe mogelijkheden. De motor van deze innovatie is het internet. In milliseconden kan informatie wereldwijd worden ontsloten en verwerkt. Dat heeft economie en maatschappij in beweging gezet. Winkelen reizen, taxivervoer, communicatie, sociale interacties en tal van andere facetten van de samenleving hebben een nieuwe inhoud gekregen.

Nederland als Europa's Digital Mainport

Nederland is zich pas recent bewust geworden van het feit dat deze innovatie ons niet overkomt, maar dat ons land zich in het centrum ervan bevindt. De basis van het internet is de digitale infrastructuur die bestaat uit faciliteiten voor grootschalig datatransport, netwerk knooppunten en datacenters met miljoenen servers. Door de aanwezigheid van de AMS-IX (Amsterdam Internet Exchange) werd Nederland het grootste internet knooppunt ter wereld. De toegankelijkheid van grootschalige internetcapaciteit, het goede vestigingsklimaat, in de wet verankerde netneutraliteit en bescherming van de Europese privacywetgeving maken Nederland een aantrekkelijke vestigingsplaats voor digitale diensten. Giganten als Google, Microsoft, Twitter, Facebook, Amazon, Netflix en Booking.com leveren thans hun diensten in Europa vanuit tientallen grote Nederlandse datacenters. Met die sterke digitale infrastructuur heeft Nederland zich in korte tijd ontwikkeld tot de digitale gateway van Europa.

Stichting Digitale Infrastructuur Nederland www.dinl.nl info@dinl.nl
Overgoo 13 - 2260AG Leidschendam @stichtingdinl +31 70 762 1070

Bovendien blijkt er een sterke correlatie te bestaan tussen een sterke digitale infrastructuur en ontwikkelingen in de economie. Daarmee heeft Nederland een uitgangspositie die enorme kansen schept![1]

Wettelijke kaders

Maar alle technologie, ook deze, heeft een keerzijde. Nieuwe ontwikkelingen brengen nieuwe risico's met zich mee. Zoals andere vormen van criminaliteit en bedreigingen voor onze persoonlijke levenssfeer. De overheid zoekt haar rol en worstelt zichtbaar met de materie. De snelheid van de ontwikkelingen maakt het voor haar moeilijk om de werkelijke aard van de verandering te doorgronden en de juiste kaders te vinden. De neiging is sterk om terug te grijpen op bestaande kaders. Dat fenomeen is niet nieuw. De eerste telefoon werd aan het eind van de 19e eeuw aangeduid als 'klanktelegraaf', en viel daarmee onder de telegrafiewet van 1854. Tot de situatie in 1904 onhoudbaar werd en de wet op communicatievoorzieningen kwam.

De geschiedenis herhaalt zich. Menig internet- en online bedrijf worden anno 2014 aangeduid als 'aanbieder van telecommunicatiediensten'. En vallen met hun activiteiten onder de Telecommunicatiewet. Opnieuw begint dat te wringen. Want de overheid claimt steeds meer ruimte in de digitale economie. Ook op plekken waar de samenleving daar grote moeite mee heeft. Voor activiteiten zoals zoals handhaving en opsporing ontbreken bruikbare kaders.

In de brief van het Ministerie van Economische zaken van 23 December 2013 aan de 2e kamer wordt gesproken over "convergentie van telecommunicatie, media en ICT". Zo wordt de groei van het internet geduid. Maar de vraag is of die uitleg klopt. Is internet een combniatie van deze drie sectoren? Of is het internet een nieuwe ontwikkeling die de media, de online- en de ICT industrie juist ingrijpend veranderd?

Een feit is dat internet en de online industrie in veel opzichten verschillen van de - in essentie - verticaal geïntegreerde wereld van de telecommunicatieindustrie, die ontstaan is uit telefonie. E-mail, whatsapp en twitter raken de telecommunicatieindustrie, Netflix en Spotify de media. Cloud raakt de ICT. Maar het internet raakt ook de hotelwereld met airBnB, en de taxiwereld met Uber.

Terug naar het thema "wettelijke kaders". Het is vreemd dat we voor zo'n enorme innovatie als internet hardnekkig een model uit het tijdperk van de vaste telefonie blijven hanteren. De vele thema's van de internetmaatschappij kunnen niet langer worden bedwongen met de gedateerde media- en

[1]Het onderzoek "Digital Infrastructure in the Netherlands, The Third Mainport", Deloitte 2013, in opdracht van DHPA, ECP, Rabo en AMS-Ix op http://www.dhpa.nl en het 2014 vervolgonderzoek op https://www.digitale-infrastructuur.nl

telecommunicatiewet. Aan de hand van concrete voorbeelden illustreren we in dit artikel waar het ontbreken van de werkbare kaders voor de online wereld en het internet, in toenemende mate wringt.

THEMA 1: SPRAAKVERWARRING

Bestudering van de recente parlementaire geschiedenis leert dat er veel onduidelijkheid bestaat over de termen en begrippen uit de digitale wereld. In debatten worden steeds nieuwe termen gebruikt om de rollen, functies en type activiteiten van internetbedrijven aan te duiden. Dit zijn steevast termen die in de telecom- en mediawet niet te vinden zijn.

Voorbeelden van zulke termen zijn “diensten van de informatiemaatschappij”, “doorgeven van elektronische content”, “internet knooppunt”, “internet service providers” of “reguliere aanbieders”. De term “internet service provider” is extra verwarrend, deze wordt zowel gebruikt om aanbieders in algemene zin te duiden als partijen die toegang bieden tot het internet.

Door het ontbreken van een goede landkaart maakt ieder zich een eigen voorstelling van die rollen. In de op zich toch al abstracte digitale wereld leidt dat begrijpelijkerwijs tot misverstanden en onduidelijke beeldvorming. Zo worden partijen die toegang bieden tot internet, in de context van auteursrechten, aangeduid als “doorgevers van content”. Dit suggereert actieve en vermengde rol bij het verspreiden van media zoals muziek of video, zoals dat in de traditionele mediawereld gebruikelijk is. De traditionele content industrie maakt bij haar verzet tegen de ontwikkelingen op het internet met regelmaat dankbaar gebruik van dat traditionele frame, door aanbieders van internet toegang medeplichtig te veronderstellen aan het schenden van auteursrechten.

In de internet wereld bestaat er juist een duidelijke, natuurlijke en noodzakelijke scheiding tussen de toegang tot het netwerk in algemene zin, en het aanbod van de daarover aangeboden diensten. Dat heeft geleid tot het principe van netneutraliteit

THEMA 2: NETNEUTRALITEIT

In 2011 besloot de kamer dat vrije en ongefilterde toegang tot het internet een fundamenteel recht is. Men ontdekte na een incident met KPN dat ongehinderde toegang tot internetdiensten samenhangt met de vrijheid van meningsuiting. Die vrije toegang werd verankerd in het principe van netneutraliteit, waarmee Nederland een voorsprong nam in de internationale discussie over dit thema.
Maar over de uitvoerbaarheid ontstaat steeds meer verwarring. Het netneutraliteitsbeginsel is ondergebracht in de telecommunicatiewet. Daarin wordt de functie van het bieden van toegang niet

precies gedefinieerd. Want die wet kent, als gezegd, geen onderscheid tussen activiteiten die te maken hebben met internet. Omdat dat voor een goede uitvoering van netneutraliteit toch nodig is, worden thans met behulp van een beleidsnotitie nieuwe termen geïntroduceerd, die het er bepaald niet eenvoudiger op maken. Zo spreekt de recente beleidsregel netneutraliteit van het Ministerie van Economische Zaken over “toegangsdiensten”, “losse diensten”, “gespecialiseerde diensten” en “content

diensten". Een combinatie van "losse diensten" wordt als "toegangsdienst" beschouwd, dat is nodig om netneutraliteit compatibel te houden met traditionele telecommunicatiediensten en -aanbieders. Op basis van deze warboel van begrippen kan geen enkele aanbieder bepalen wat hij nu wél of niet mag, zonder eerst een jurist te raadplegen. Concrete vragen uit de sector worden door het Ministerie van Economische Zaken doorgeschoven naar het ACM, die mag zich er nu verder over buigen. Een beter voorbeeld van onnodige toename van lasten- en regeldruk is bijna niet te vinden.

Met een landkaart voor internetactiviteiten, die wij later zullen introduceren, is deze kwestie eenvoudig op te lossen.

THEMA 3: PRIVACY

De Wet bescherming persoonsgegevens (Wbp) beschermt onze privacy. In de Wbp staat wat er wel en niet mag met persoonsgegevens incl. het recht van de betrokkene als zijn gegevens worden gebruikt. Denk aan het recht op informatie, inzage en op verzet tegen gebruik van gegevens.

De Wbp kent als basisbegrippen de rol van *betrokkene* (de persoon wiens gegevens het betreft), de *verantwoordelijke* (de partij die de informatie rechtstreeks van de betrokkene ontvangt) en de *bewerker* (een partij die namens de verantwoordelijke data verwerkt). Het op de traditionele ICT praktijk gebaseerde beeld is dat de verantwoordelijke de volledige regie heeft over de gegevens, en de bewerker kan opdragen wat er wel of niet mag.

Maar de complexe praktijk van het internet, waar altijd sprake is van lange en complexe ketens van veel betrokken partijen, werkt heel anders. Verantwoordelijken hebben geen zeggenschap over bewerkers, die een eigen beleid hebben met betrekking tot hun dienstverlening. De verantwoordelijke online dienstverleners maken altijd gebruik van diensten van anderen. Zoals datacenters, hosters en de aanbieders van de uiteindelijke applicaties of sites. In de praktijk worden dan ook nooit bewerkersovereenkomsten afgesloten, laat staan gecontroleerd. Actief naleven van die verplichting zou neerkomen op, wederom, een toename van administratieve lastendruk. En ook hier biedt de telecommunicatiewet geen uitkomst.

Een kader en landkaart dat in één oogopslag laat zien wie in de wereld van het internet de rol van de verantwoordelijke en die van de bewerker heeft incl. de geldende basisverplichtingen voor bewerkers, zou een grote bijdrage en verbetering kunnen leveren aan het daadwerkelijk borgen van onze privacy.

THEMA 4: ZORGPLICHT

Minister Kamp kondigde in de eerder genoemde kamerbrief een uitbreiding van de zorgplicht aan. Die zou "moeten worden uitgebreid naar andere aanbieders in het internet waardeweb". Dat is geen vreemde gedachte nu de samenleving in korte tijd enorm afhankelijk is geworden van het goed en veilig functioneren van online diensten.

Los van het feit dat niet helder is welke aanbieders dat dan zou moeten betreffen, is het maar de vraag of de telecommunicatiewet hier als uitgangspunt zou moeten dienen. Dat heeft potentieel schadelijke neveneffecten. De grofmazige telecommunicatiewet zou bijvoorbeeld de AMS-IX, het grootste internetknooppunt ter wereld, in principe kunnen verplichten om verkeersinformatie op te slaan en filteren of tappen te faciliteren. Dat terwijl AMS-IX niets van doen heeft met deze informatie en slechts verbindingen faciliteert. Die netneutrale, logistieke positie is juist één van de redenen van hun succes en geeft Nederland een sterke positie in de wereldwijde online economie. De AMS-IX opzadelen met informatieplichten zal het vertrouwen flink schaden, en daarmee dus onze economie.

THEMA 5: HET MKB KEURMERK "VEILIG INTERNET"

Een ander thema uit de eerder genoemde visiebrief telecommunicatie en internet, is het "keurmerk voor veilige internetdiensten voor het MKB". Net als de zorgplicht, is een keurmerk geen onlogische gedachte.

Bedrijven hebben behoefte aan duidelijkheid over de betrouwbaarheid van dienstverlening en het veilig beheren van hun gegevens. Er zijn zorgen over cloud computing en de locatie van data. Gegevens behoren goed te worden beschermd tegen toegang door onbevoegden. In de oude ICT wereld volstond een eenvoudige controle, want de IT Manager van een bedrijf had de regie over zijn gehele systeem of werkte met onderaannemers.

Jammer genoeg is de term "keurmerk" ongelukkig gekozen. Er zijn veel keurmerken en certificaten, die vaak flinterdun zijn, deze zijn veelal gebaseerd op een eenvoudige vragenlijst. Of simpelweg te koop door toetreding tot een organisatie. Er is nog een groot nadeel: de meeste certificaten of keurmerken hebben betrekking op één onderdeel van de dienstverlening.

Ter illustratie: Een modern datacenter van waaruit internetdiensten worden geleverd krijgt jaarlijks vele keren bezoek van verschillende auditors, gestuurd door verschillende opdrachtgevers die elk iets willen weten over de veiligheid en betrouwbaarheid. Ze concluderen allemaal dat het datacenter een goede fysieke toegangsbeveiliging heeft. Maar over de informatieveiligheid van de gehele online dienst zegt dat uiteraard niets. Bij wie moeten ze nog meer controleren?

Kortom: certificering en controle van een enkele partij voldoet niet meer als kwaliteitsinstrument voor internetdiensten. Alle partijen die betrokken zijn in online ketens moeten veilig en betrouwbaar zijn om het geheel, de dienst waar het om gaat, van zekerheden te kunnen voorzien. Elke keten is immers zo zwak als de zwakste schakel.

Om een keten veilig te maken moet men eerst de verschillende schakels kunnen benoemen. Zonder de eerder genoemde landkaart en een bijbehorende opzet voor de plichten van elk van de spelers met betrekking tot bijvoorbeeld informatiebeveiliging, heeft een dergelijk keurmerk geen enkele waarde. Het

zal in deze situatie leiden tot veel dubbel werk en hoge kosten. Met als netto resultaat een flinke verzwaring van de administratieve lasten en een forse kans dat het gewenste doel niet wordt bereikt.

THEMA 6: HANDHAVING EN OPSPORING

Ook bij het bestrijden van internetcriminaliteit levert het ontbreken van een bruikbaar kader problemen op, dit knaagt rechtstreeks aan het vertrouwen in de gehele digitale economie.

Bij het bestrijden van jihadistische uitingen op het internet, of het verwijderen van frauduleuze activiteiten is het voor justitie niet bij voorbaat helder in welke hoedanigheid een internetbedrijf handelt. Gaat het om een rechtspersoon die de uitingen zelf heeft geplaatst en ook verantwoordelijk is voor de techniek? Of is het een bedrijf dat slechts de technologie biedt om uitingen te plaatsen? Of is het een bedrijf dat alleen toegang biedt tot het internet, en netneutraal moet opereren?

Bij het vergelijken van de diverse arresten, uitspraken etc. wordt duidelijk dat uniformiteit van aanpak ver te zoeken is. Dat is niet verwonderlijk, een goed overzicht en een definitie van de activiteiten van betrokken partijen in de keten ontbreekt.

Het wetsvoorstel computercriminaliteit III hanteert als basisbegrip zelfs de term “geautomatiseerd werk”. Dat omvat álle informatietechnologie, in de ruimste zin van het woord. De vraag dient zich aan of het niet noodzakelijk is om ook hier onderscheid te maken tussen type activiteiten. Een mobiele telefoon van een crimineel is echt iets anders dan een centrale faciliteit waarmee de werking van het gehele internet kan worden verstoord. Of de systemen van een kerncentrale.

De politiek zou in beginsel een instrument moeten hebben om die rollen en type activiteiten aan te kunnen duiden. Hiermee kan een goede afweging worden gemaakt tussen de wenselijkheid van handhaving of opsporing. Daarmee worden de risico’s voor economie en samenleving bij autonoom ingrijpen van Justitie, en de risico’s voor het vertrouwen in de online economie duidelijker. De term “geautomatiseerd werk” is dan naar alle maatstaven een veel te botte.

SAMENGEVAT: TIJD VOOR NIEUWE KADERS EN BEGRIPPEN

Voor alle belangrijke infrastructuur in de samenleving bestaat een wettelijk kader. Voor elektriciteit, water, wegen, luchtvaart, media en ook voor communicatie. Maar niet voor het internet. De gehele digitale economie afdoen als een vorm communicatie is niet langer werkbaar.

De Minister van Economische Zaken spreekt in zijn visiebrief van 23 december 2013 al over een dergelijk kader, dat hij het “Internet Waardeweb” noemt. Het ministerie heeft dus een aanzet gemaakt en dat is op zich te prijzen. Maar het voorgestelde model voldoet niet. Het leunt op begrippen uit de media- en telecomwereld en probeert die in het model te verwerken.

Een echt goed kader, we noemen het alvast “de Datawet”, is nu hard nodig. Daarmee kunnen we duidelijkheid scheppen in de debatten over de goede en ook de slechte dingen die op ons afkomen. Met de Datawet kunnen we betere afspraken vastleggen over de online wereld. Zo kunnen we precies aangeven welke regels en afspraken voor wie gaan gelden en voor wie niet. Met een goede Datawet zetten we als internetland de toon en kunnen we weer tientallen jaren vooruit!

Stichting Digitale
Infrastructuur Nederland

De Datawet

Een goede wet begint met een helder kader, definities en inzicht in de rollen en functies in het geadresseerde thema. Een nieuw kader voor het internet, we noemen het “de Datawet”, legt vervolgens bij elk van die rollen de behorende verplichtingen, beperkingen en rechten vast. De Datawet geeft de samenleving, de economie en overheid daarmee de mogelijkheid om activiteiten, verantwoordelijkheden, verplichtingen en risico’s scherp vast te stellen.

Met de Datawet in de hand weten betrokken bedrijven direct bij welke van hun activiteiten ze rekening moeten houden met specifieke regels. Dat maatwerk voor het internet zorgt voor betere uitvoerbaarheid, controle en toezicht, en daarmee tot vermindering van regel- en lastendruk voor zowel overheid als bedrijven. De Datawet legt verbindingen met Wbp, met de telecommunicatiewereld, geeft begrippenkaders voor handhaving en opsporing en beschermt kritieke infrastructuur.

De gangbare opinie vanuit de internetgemeenschap is dat wettelijke kaders en regels onwenselijk zijn. Het internet is vrij en open. Wetten, regels en overheidsbemoeienis zijn ongewenst. Die intentie is absoluut waar. Niemand zit te wachten op een klassieke “markt” regulering van het internet. Maar tegelijkertijd kan de overheid niet aan de kant blijven staan. De opsomming van thema’s in de eerdere paragrafen geven aan dat de overheidsbemoeienis hoe dan ook toeneemt. Want als digitale burgers willen we ook bescherming van onze rechten en een optreden van de overheid tegen cyber criminelen. Daarvoor zijn, als gezegd, moderne kaders nodig. De essentie van de Datawet is niet regulering, maar kan door haar opzet juist bewegingen uit de telecommunicatie-industrie die naar regulering neigen, helpen voorkomen

De behoefte aan een Datawet is internationaal. Er is geen precedent. Omdat de Datawet op zich niets verandert aan de al bestaande ingezette rechten en plichten maar slechts nieuwe definities en kaders stelt, is er geen reden om aan te nemen dat dit grote conflicten oplevert. De Datawet gaat niet over nieuwe regels, maar over nieuwe kaders en definities.

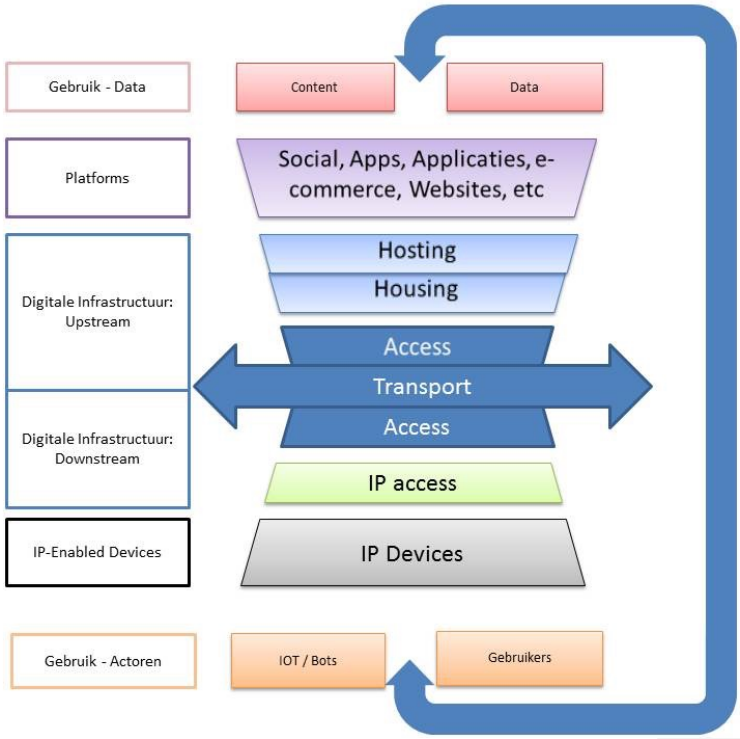
De Datawet legt vast welke rechten door wie moeten worden beschermd, welke plichten gelden voor partijen in de keten en waar politie iets te zoeken heeft - en waar niet.

De Datawet biedt Nederland een kans om als land met een enorm grote rol in het wereldwijde internet, de toon te zetten in het debat over governance, plichten, rechten en werking. Zo neemt Nederland ook hier het initiatief, wijst de weg en vergroot daarmee de voorsprong als leidend land in de internationale digitale economie.

LANDKAART

Bedrijven en organisaties in de online wereld hanteren al meer dan 20 jaar een begrippenkader dat zijn wortels heeft in de historie van het internet. Die landkaart is echter nooit geformaliseerd. De DHPA heeft thans het initiatief genomen om deze landkaart te gaan tekenen.

Het kernthema van de Datawet is onderstaande landkaart, deze geeft essentiële functies en activiteiten van de internet wereld weer.



Het uitgangspunt van deze landkaart is een indeling in functies. Functies kennen karakteristieken, en bijbehorende rechten en plichten. In de praktijk worden de getoonde functies vaak ingevuld door gespecialiseerde partijen. Maar ook zijn er partijen die meerdere functies aanbieden. Ter illustratie: een fabriek die een restaurant exploiteert moet zich houden aan de voedsel- en warenwet. Daarmee wordt die fabriek niet meteen een horecabedrijf. In de leveringsketens van het internet vinden we ook stichtingen en verenigingen, zoals de vereniging AMS-IX.

De DHPA kiest voor het (aansluiten bij) gangbare Engelstalige terminologie. Dat sluit aan bij de praktijk, want in de Nederlandse taal zijn nauwelijks (bruikbare) termen ontstaan of ontwikkeld voor de activiteiten in de online wereld. Daar zal de Datawet geen verandering in kunnen brengen.
De voorgestelde Indeling biedt slechts een aanzet voor verdere discussie. De impact van een nieuw kader is groot en ongetwijfeld zal verdere verdieping nodig zijn.

De landkaart kent de volgende elementaire blokken:

1. Gebruik;
2. IP- Devices;
3. Digitale Infrastructuur Downstream;
4. Digitale Infrastructuur Upstream;
5. Platforms.

Stichting Digitale
Infrastructuur Nederland

GEBRUIK

Het internet en al zijn toepassingen wordt gebruikt door zakelijke- en/of privé gebruikers. Er komt echter steeds meer aanleiding om ook de rol van niet-menselijke gebruikers te benadrukken: we noemen dit de BOT. Voorbeelden van BOTs zijn automatische thermostaten, Google's auto en straks misschien ook de virtuele, softwarematige kinderen die worden ingezet voor opsporing van kindermisbruik. Ook kan het gaan om apparaten die door een infectie zijn gerekruteerd voor het gebruik in een BOt-net. Voor deze categorie wordt ook de term IOT (Internet of Things) gebruikt, al is er een subtiel maar belangrijk verschil: de benoemde BOT-rol gaat over gedrag, niet over technologie.

Gebruikers, menselijk of automaat, ontvangen en verzenden data - die wordt getransporteerd, verwerkt en/of opgeslagen door de vele andere functies in de internetketen. Content betreft data die kan zijn beschermd door auteursrechten. Data, indien deze betrekking heeft op een persoon, kan zijn onderworpen aan privacywetgeving en de Wbp. Andere data kan zijn onderworpen aan bescherming/ vertrouwelijkheid – in de vorm van een zorgplicht.

De relatie tussen gebruikers/BOTs en de door hen ontvangen of verzonden data is zowel juridisch (de dikke pijl op de landkaart) als technisch (getransporteerd en verwerkt door de stapel van diensten). Deze paden zijn tegengesteld.

IP-DEVICES

IP-Devices zijn apparaten die onder regie van een gebruiker zijn aangesloten op het internet. Voorbeelden zijn PC's, tablets, routers, smart TV's, mobiele telefoons. Het betreft hier dan de hardware en basis functies van het device.

DIGITALE INFRASTRUCTUUR - DOWNSTREAM

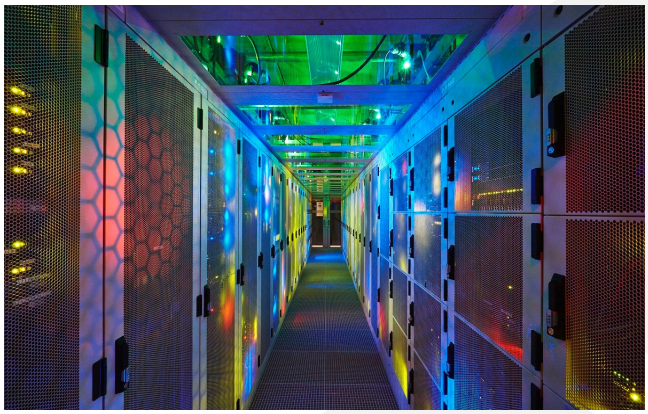
We onderscheiden, net zoals bij de productie van fossiele brandstoffen, de termen *Upstream* en *Downstream*. Dat onderscheid is nodig om het verschil in functie aan te brengen, waar de techniek zelf het onderscheid niet maakt.

Downstream omvat de netwerkfuncties aan de kant van het gebruik van de online wereld. Downstream functies zorgen ervoor dat de gebruikers/BOTs de apparatuur onder hun regie (IP-Devices) kunnen aansluiten op het internet en gebruik kunnen maken van diensten aan de Upstream kant.
De sub-functie "IP-Access" staat momenteel vaak bekend als "ISP", dit is de functie waarmee (de apparatuur van) de gebruiker is aangesloten op het internet. en de functie waar de netneutraliteitsdiscussie zich feitelijk op toespitst.

De sub functie “Access”, betreft de fysieke toegang: kabel, glasvezel, 3G /4G of publieke Wi-Fi die het IP-enabled device en vervolgens de gebruiker fysiek verbindt met het internet. Deze functie is slechts netneutraal waar dit het transport van internet betreft (IPv4 of IPv6). Dit omdat deze functie veelal wordt gedeeld met diensten in de traditionele media- en telecommunicatie-industrie zoals TV en traditionele telefonie. Deze vallen buiten het bestek van deze landkaart.

DIGITALE INFRASTRUCTUUR – UPSTREAM

De Upstream kant betreft de netwerkactiviteiten aan de productiekant van de online wereld. De upstream functie ontsluit het internet voor die platforms. De Upstream functie kent, net zoals de downstream kant, de sub functie “Access”: waarmee de functies Hosting en Housing op het hart van het internet worden aangesloten.



We onderscheiden de functies Housing, de fysieke locatie van waaruit online diensten worden geleverd, en Hosting, de aanbieders van hardware en basis-software voor het faciliteren van platforms. Mogelijk is hier nog onderscheid tussen hardware en software van belang.

In het hart van het internet vinden we de pure transport functies zoals Peering en de Internet Exchanges. Dit zijn de plaatsen waar de fysieke circuits van de Upstream en Downstream activiteiten elkaar ontmoeten. Het mag duidelijk zijn dat deze functie voornamelijk een logistieke betekenis heeft voor de online economie.

PLATFORMS

De functie platforms is waar het in het internet eigenlijk allemaal om draait. Hier vinden we o.a. e-commerce, websites, apps, de verwerking van big data, zoekmachines, social media en aanbieders van media. Het zijn de platforms waaraan gebruikers hun data toevertrouwen, of waaruit ze hun data of media verkrijgen.

Dat betekent dat eisen als keurmerken, zorgplicht en privacy altijd het eerste raakvlak hebben in een platform. Daar worden de eisen manifest en kunnen sectorspecifieke regels of verplichtingen gelden met betrekking tot het niveau van bescherming van informatie.

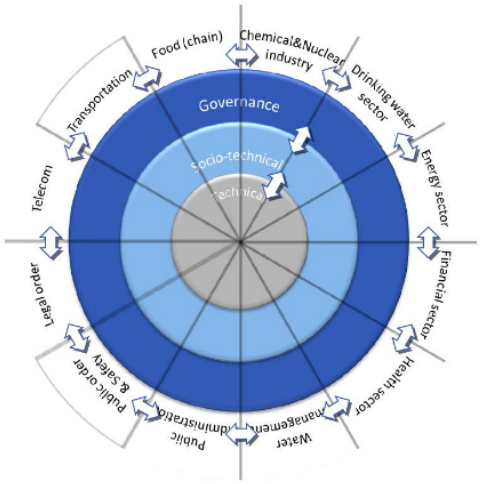


Figure 1: Conceptualization of *cyberspace* in *layers* and (cyber) *sub-domains*.

Dit mechanisme, de matching van socio-economische en sectorspecifieke waarden naar diensten in de online economie, is goed beschreven door TU Delft hoogleraar Jan van de Berg in zijn prijswinnende paper over cyberspace[2]. Met betrekking tot dit paper kan de landkaart worden gezien als een uitwerking van de socio-technical layer. De Datawet als geheel als de governance layer.

Een belangrijke overweging is dat, in principe, vrijwel alle andere rollen in de landkaart agnostisch zijn ten opzichte van de platforms en hun toepassingen. Voor een datacenter (Housing) dat allerlei verschillende platforms moet herbergen zal een grootste gemene deler gelden voor wat betreft informatieveiligheid. Het resultaat is een generieke basisbescherming van hoog niveau voor rollen in de landkaart – een beweging die bij een aantal van de genoemde spelers al volop is ingezet.

[2] "On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education"

Stichting Digitale
Infrastructuur Nederland

Voorbeelden van toepassing van de Datawet

De Datawet verschaft als gezegd duidelijkheid over de plichten, rechten en verantwoordelijkheden die horen bij elk van de genoemde functies in de landkaart. Aan de hand van de eerder genoemde voorbeelden illustreren we hoe de Datawet helderheid kan brengen in elk van die situaties.

NETNEUTRALITEIT

Netneutraliteit is van toepassing op alle “blauwe” blokken (upstream en downstream transport en access), en de IP-access. Netneutraliteit beschermt de rechten van gebruikers/BOTs voor toegang tot upstream functies. Maar ook de toegang tot andere gebruikers/BOTs en platforms en de rechten en plichten van aanbieders ten opzichte van elk van de andere functies. Zo kunnen ook de technische uitzonderingen voor internetverkeer, bijvoorbeeld het gewenste gedrag bij overbelasting, goed worden beschreven, zonder risico op conflicten met de telecommunicatiewet. [3]

Ook kan de netneutrale interactie met platforms worden geadresseerd. Ter illustratie: netneutraliteit in deze opzet kan duidelijkheid geven over de al dan niet toegelaten (commerciële) afspraken tussen een platformaanbieder en een IP-access aanbieder.

ZORGPLICHT

Een zorgplicht zal kunnen gelden voor de functies transport en access, alsmede voor specifieke upstream- en platformfuncties die zijn aangewezen als kritieke infrastructuur. Als illustratief voorbeeld: upstream en platformpartijen die betrokken zijn bij het functioneren van de watervoorziening moeten faciliteiten bieden die een bepaalde mate van beschikbaarheid of continuïteit moeten garanderen. Voor elk van de functionele blokken kan een reeks van garanties worden opgelegd voor beschikbaarheid en veiligheid. Voor andere functies geldt de zorgplicht dus niet.

BEWAARPLICHT EN TAPVERPLICHTING

De bewaarplicht (opslag van verkeersgegevens) is in Nederland van van toepassing voor 'aanbieders van openbare telecommunicatiediensten. Het Hof van Justitie, en vervolgend de Raad van State hebben zich uitgesproken tegen deze verplichting. Dat neemt niet weg dat er voor Justitie in geval van verdenking of in het belang van opsporing de noodzaak kan bestaan om specifieke informatie tot haar beschikking te hebben. Gedacht kan worden aan een andere invulling van zogenaamde 126A verzoeken, waarbij de aanbieder van IP-acces of de betreffende platform aanbieder een verplichting krijgt opgelegd om aan specifieke informatieverzoeken te voldoen binnen een gestelde termijn. Het is dan aan de aanbieder om te bepalen hoe die verplichting, met bijvoorbeeld de centrale afhandelingsfaciliteit van het NBIP, kan worden ingevuld.

Die verplichting is dan ook niet langer van toepassing op andere functies. Daarmee wordt direct duidelijk aan welke partijen de overheid informatieplichten kan opleggen en aan wie niet. Dat kan het vertrouwen en transparantie in de gehele internet economie zal vergroten.

[3] DHPA reactie op de beleidsnotitie Netneutraliteit, met een overzicht van al-dan-niet toegelaten activiteiten

PRIVACY EN WBP

De Datawet landkaart zorgt voor een vereenvoudiging van de uitvoering van de Wbp en de Europese dataprotectie directieven.

De Wbp spreekt over de betrokkene, de verantwoordelijke en de bewerker. In dit Datawet schema is de gebruiker de betrokkene, de platforms zijn altijd de verantwoordelijke en alle andere partijen zijn bewerkers. In deze opzet kan dus worden volstaan met standaard regels voor alle bewerkers die te maken hebben of zouden kunnen hebben met persoonsgegevens: i.e. het bieden van adequate informatiebeveiliging en een verbod om gegevens aan derden ter beschikking te stellen zonder toestemming van de betrokkene.

In deze opzet kan het hele gedoe met bewerkersovereenkomsten tussen partijen achterwege blijven, hetgeen de lastendruk flink zal verminderen. Ook biedt deze aanpak een oplossing voor de precaire discussies over opslag van persoonsgegevens (zoals medische gegevens); omdat alle bewerkers onder één streng beveiligingsregime zullen vallen en dus vergelijkbare maatregelen zullen moeten treffen voor bescherming.

Hoe scherper de te nemen maatregelen per functie worden afgestemd op het doel van gegevensbescherming, hoe eenvoudiger de uitvoering van de Wbp zal worden. Het leidt tot een beter resultaat: bescherming van de privacy en een betere vergelijking tussen partijen.

Ook de meldingsplicht wordt eenvoudiger uitvoerbaar. In de keten is nu immers direct te zien wie bij een security breach aan wie moet melden: downstream aanbieders aan de gebruiker, en de upstream provider aan de platforms – en die op diens beurt aan de gebruiker.

KEURMERK VEILIG ONLINE

Het eerder genoemde keurmerk zou moeten bijdragen aan het realiseren van informatieveiligheid in de online ketens. Ook hier is de Datawet-landkaart randvoorwaardelijk. Want de risico's voor toegang door onbevoegden zijn voor elk van de partijen in de landkaart verschillend en kennen elk een eigen veiligheidsregime.
Ter illustratie: de functie housing heeft te maken met fysieke risico's maar voor de functie platform gaat het uitsluitend om een logische toegang tot gegevens.

Met de hulp van de landkaart kunnen maatregelen veel beter worden afgestemd op de specifieke risico's van de betrokken partijen. Voor elk van de functies kan een "minimum-adequate" lijst van beschermingsmaatregelen op worden opgesteld, op basis van bestaande internationale standaards. Als iedere partij deze maatregelen verzorgt wordt daarmee de gehele online keten veiliger en kan die veiligheid ook inzichtelijk worden gemaakt. Zo wordt voorkomen dat partijen met onnodige, voor hen niet relevante regels en verplichtingen worden geconfronteerd. Tegelijkertijd wordt het resultaat, een veilige dienstverlening, zonder toename van de regeldruk, bereikt

HANDHAVING EN OPSPORING

De Datawet biedt eveneens een helder perspectief voor de aanpak van handhaving en opsporing. Enerzijds van gebruikers en anderzijds van strafbaar gedrag van eigenaren van andere functies in het schema.

Van belang is dat daarbij de platforms en de up- en dowstream functies, het hart van het internet, moeten worden beschermd tegen de (willekeurige) toegang door opsporingsdiensten indien er (slechts) sprake is van strafbaar gedrag van een gebruiker. Bij de opsporing van zulke gebruikers kan het nodig zijn om toegang te verkrijgen tot data of verkeersgegevens die vergaard zijn onder bewaarplicht of tapverplichting. Ook is het denkbaar dat Justitie het recht zal krijgen om zich toegang te verschaffen tot IP-devices die eigendom zijn van die gebruiker, i.e. de (rechts) persoon die verdacht wordt van bepaalde strafbare feiten.

Het is Justitie dan dus niet toegestaan zich toegang te verschaffen tot bijvoorbeeld de upstream-functies, als een eigenaar of gebruiker van een platform dat gebaseerd is op die upstream functies, een strafbaar feit zou plegen. Daarvoor volstaat dan de veelgenoemde “54a” procedure.

Als dat scherpe onderscheid bestaat, kan eventueel worden nagedacht over een beleid waarbij Justitie zich toegang mag verschaffen tot een upstream functie als er sprake is van aan het internet-gerelateerd strafbaar gedrag door de rechtspersoon die eigenaar is van die betreffende functie. Bijvoorbeeld: een housing aanbieder die zelf verdacht wordt van het actief meewerken aan verspreiding van kinderporno, is niet gevrijwaard van ingrijpen door justitie.

Het schema biedt een helder perspectief op de aanpak voor het verwijderen van onrechtmatige content, namelijk de Notice en action. In eerste instantie zal de gebruiker moeten worden benaderd en opgedragen om dit te verwijderen. Als deze gebruiker niet te traceren of niet te bewegen is tot verwijdering, zal de volgende functie, de platformeigenaar, moeten worden benaderd. Als laatste escalatiemogelijkheid kan de hoster worden benaderd. Slechts als deze hoster niet meewerkt of niet reageert, kan Justitie op grond van het eerder genoemde beginsel dat deze dan strafbaar is, actie ondernemen richting de eigenaar van genoemde functies. Alle andere functies zijn uitgesloten. Voor verwijdering van content kunnen andere up- en downstream functies nooit worden aangesproken, zodat het vertrouwen en de beschikbaarheid van het internet in alle gevallen wordt gewaarborgd.

DATA PORTABILITEIT (EU THEMA)

In de relatie van gebruikers naar platforms, en platforms naar upstream providers (hosters) kan worden vastgelegd dat data overdraagbaar en opvraagbaar moet kunnen zijn. De Datawet beperkt de impact van data portabiliteit dan tot deze functies. Voor andere functies is deze thematiek niet relevant.

Stichting Digitale
Infrastructuur Nederland

Afsluitend

Dit document schetst een visie op een nieuw wettelijk kader voor het internet en is bedoeld als een aanzet voor verdere discussie. Geen enkele grote wijziging in kaders is zonder risico's. Er moet rekening worden gehouden met bestaande praktijken en regels.

Er zijn ongetwijfeld details die een nadere uitwerking vereisen. Dat zal ons niet moeten weerhouden van de ambitie om een richting in te slaan die de online economie, met in het bijzonder de positie van Nederland, op een nog nauwelijks in te halen voorsprong zet. Nederland kan dan worden gezien als thought-leader over wereldwijde thema's zoals privacy, kwaliteit en bescherming tegen- en bestrijding van cybercrime.

De Datawet: het gereedschap voor de toekomst!

Hoe nu verder?

Dit document is tot stand gekomen op basis vele discussies met- en bij betrokken partijen in de internet wereld waaronder ECP, SIDN, AMS-IX, NLnet, NIP, SURF, ISPconnect, ISOC, Ministerie van Economische Zaken, Ministerie van Justitie, WODC, WRR en vele anderen.

Een verdere uitwerking zal tot stand moeten komen met de overheid, wetenschap en vele organisaties in de online sector.

November 2014
Michiel Steltman | Directeur DINL

Stichting Digitale
Infrastructuur Nederland

Q&A

***Q:* Is het niet zo dat Nederland een dergelijk initiatief als de Datawet niet op eigen houtje zou moeten nemen, maar zou moeten wachten op een initiatief uit de EU?**

A: Nederland blijkt in allerlei opzichten voorop te lopen bij de diverse discussies over het internet. Zoals over NTD, handhaving en opsporing, de eerder genoemde convergentie (i.e. ontwikkelingen m.b.t. het waardeweb). Een discussie over een nieuw wettelijk kader voor het internet uit Brussel is op korte termijn niet te verwachten. We mogen er van uitgaan dat een aanzet voor een werkbaar kader door de EU kan worden overgenomen.

Bovendien zal de Datawet in voorgestelde vorm geen conflicten opleveren met bestaande wettelijke kaders, de Datawet zal juist helpen om ingeslagen wegen beter te bewandelen en de huidige praktijk te verduidelijken en vereenvoudigen.

***Q:* Leidt de Datawet niet tot regulering van het internet?**

A: De essentie van de Datawet is niet regulering maar kan door haar opzet juist bewegingen uit de telecommunicatie-industrie die naar regulering neigen, helpen voorkomen. De Datawet is toegesneden op het internet en biedt kaders die een praktische en scherpe invulling geven aan praktijken rond het internet die thans aan de telecommunicatiewetgeving worden toegevoegd en die ongewenste neveneffecten hebben. In die zin beschermt de Datawet juist de vrijheid en neutraliteit van het internet.

***Q:* Het internet is in essentie toch een vorm van telecommunicatie?**

A: Dat mag zo lijken maar de telecommunicatie-industrie heeft zich in de afgelopen 100 jaar in een compleet andere richting ontwikkeld dan het moderne internet. De complexiteit en realiteit van het internet wordt geen recht gedaan met een wettelijk kader dat niet meer past en de groei en ontwikkeling ervan zal remmen.

***Q:* Wetten moeten gemaakt worden voor een lange termijn. Het internet verandert snel, is een Datawet dan wel verstandig?**

A: De diensten op het internet veranderen inderdaad snel maar het internet zelf bestaat in de vorm als geschetst in de landkaart al zo'n 25 jaar. In die periode zijn de rollen en functies niet fundamenteel gewijzigd.