In navolging op onze informatieavond Algemene Verordening Gegevensbescherming vond op donderdag 20 oktober de tweede EU privacybijeenkomst van de werkgroep privacy plaats.

Leden van de werkgroep privacy hadden stellingen bedacht rondom een aantal belangrijke privacythema's die deze avond centraal stond.
- De Algemene Verordening Gegevensbescherming
- De opslag van medische gegevens in de cloud
- De hack-bevoegdheid door de politie in de Wet computercriminaliteit III

Een panel van deskundigen reageerden vanuit hun expertise en ervaring op deze stellingen. Daarnaast was er gelegenheid voor het publiek om te reageren en vragen te stellen aan het panel.

Voorstelronde
In het panel zaten:

Romeo Kadir, algemeen directeur Stichting Privacy Nederland, een erkende ANBI, en directeur van het Nederlands Privacy Compliance Instituut (NPCI), welke zich tot doel stellen om de privacy en dataprotectie in Nederland te bevorderen.
Romeo: De kern is dat we dit alleen met elkaar kunnen doen door te realiseren dat privacy een 'quality of life' is en door het stimuleren van een kritische massa.
De stichting staat voor de eerbieding van de persoonlijke levenssfeer zoals deze in de grondwet is bepaald. Romeo Kadir is bij verschillende ondernemingen privacy compliance officer geweest. Deze functie stond in het teken van het respecteren en effectueren van privacyregels en het bevorderen van 'awareness' rondom privacy.

Jochem de Groot is Government Affairs Manager voor Microsoft in de Beneluxlanden. Namens Microsoft is Jochem het eerste aanspreekpunt voor politiek, overheid en het maatschappelijk middenveld over beleidskwesties op het snijvlak van technologie en privacy (protectie) en (cyber) security. Tot 2013 was Jochem de Groot beleidsadviseur internetvrijheid en mensenrechten bij het Ministerie van Buitenlandse Zaken. Hem valt op dat discussies over gegevensbescherming in een stroomversnelling zijn geraakt sinds de onthullingen van Edward Snowden. Privacy maakt sindsdien een versterkte ontwikkeling door die ook merkbaar is bij bedrijven, zoals Microsoft.

Nico van Eijk is hoogleraar Informatierecht, Media- en Telecommunicatierecht aan de Faculteit der Rechtsgeleerdheid van de universiteit van Amsterdam.
Nico: Regelgeving op het gebied van de media en telecommunicatie is permanent in beweging als gevolg van snelle technologische ontwikkelingen. Fundamentele uitgangspunten als de vrijheid van meningsuiting en privacy mogen daarbij niet uit het oog worden verloren.
Nico van Eijk schreef mee aan een onderzoeksverslag over de complicaties van de USA Patriot-act al voordat Snowden zijn onthullingen deed over het massaal verzamelen van data.

In de VS gelden andere regels voor het verzamelen en gebruik van persoonsgegevens dan in de EU. De continenten proberen elkaar slechts te overtuigen van hun eigen gelijk. Er bestaan ook veel misverstanden over en weer. Volgens Nico van Eijk zou het beter zijn zich niet alleen te focussen op de verschillen, maar te zoeken naar een meer praktisch samenwerking tussen beide continenten.

De Algemene Verordening Gegevensbescherming (hierna: AVG)
Onze voorzitter start de paneldiscussie met de opmerking dat de AVG niet door iedereen positief ontvangen is. Het is de zwaarst belobbyde Europese wetgeving ooit met 4000 – 1 amendementen.
Veel gehoorde kritiek op de AVG :
1. Not in my backyard: Sectoren zien liever niet dat de privacy bepalingen op hen van toepassing zijn en willen graag onder een uitzondering vallen.
2. De AVG richt elke vorm van innovatie en vooruitgang ten gronde door de strikte voorschriften in de verordening.
3. Implementatie van de AVG kost bedrijven teveel geld.

Stelling I:
Hoe kijken de panelleden aan tegen de AVG?
Romeo Kadir: Is positief over de AVG. Romeo legt de nadruk op de betekenis van privacy in het dagelijks leven. Bedrijven redeneren nu vooral dat privacy een belangrijk onderwerp is MAAR…> Dat zal moeten veranderen naar privacy is heel belangrijk DUS. Het uitgangspunt moet zijn dat 'personal life' gerespecteerd moet worden, de AVG zal dit vergroten. Daarnaast verplicht de AVG bedrijven tot een sterkere privacy awareness. Romeo gaat kort in op de preambule en het verhoogde klachtrecht van de AVG.

Jochem de Groot: vraagt zich af of nieuwe wetgeving, zoals de AVG op langer termijn wel houdbaar is omdat de technologische ontwikkelingen erg snel gaan. De vraag is dan ook hoe eigenaarschap van data op de langere termijn geborgd blijft. Beleidsmakers en politici moeten digitaal beleid maken waarbij er een balans is tussen de veiligheid en vrijheid van burgers. Microsoft heeft een bijdrage geleverd aan het maatschappelijk debat hoe dit gebalanceerd digitaal beleid eruit moet zien, door het boek: 'A Cloud for Global Good' : https://news.microsoft.com/cloudforgood/
In dit boek wordt beschreven welke uitgangspunten van belang zijn bij het vormgeven van digitaal beleid door politici, overheden en bedrijven, zodat grondrechten worden gerespecteerd en maatschappelijke ongelijkheid wordt voorkomen.

Problemen voorziet Jochem de Groot bij de implementatie van de AVG. De verordening geeft lidstaten ruimte voor een eigen lokale uitleg. Er ontstaan daardoor onderling veel verschillen tussen de uitleg en toepassing van privacyregels tussen de lidstaten. Jochem: Blijft er dan wel een level playing field over? Ook zullen er grote verschillen ontstaan bij de handhaving van privacyregels door de verschillende toezichthouders binnen de EU.

Nico van Eijk vindt de AVG weinig geslaagd. Het document mist flexibiliteit, het heeft een te groot aantal bepalingen terwijl het belangrijke thema's zoals daadwerkelijke handhaving laat liggen. Daarnaast wordt het onderwerp privacy in de verordening 'gecommercialiseerd'. Er worden zaken in de verordening geregeld waar ook al algemene regels voor zijn, zoals consumentenrecht, arbeidsrecht en marktregels. De AVG is desalniettemin een mooie uitdaging voor advocaten en juridisch adviseurs door de ingewikkelde regelgeving. In de praktijk zal het lang duren voordat de Europese toezichthouders dit op orde hebben. Juridische procedures kunnen vele jaren nemen. Bedrijven die zich niet aan de wet houden kunnen in de tussentijd gewoon hun gang gaan. De EU kan veel leren van de Amerikaanse traditie met betrekking tot privacyhandhaving.

Nico: De vraag zou moeten zijn wat willen we precies met deze wetgeving bereiken? Wat is het doel van de privacyregels en hoe handhaven we ze?
Een alternatief voor de AVG is een normatief regelgevend kader met slechts een paar bepalingen.

Jochem de Groot en Nico van Eijk zijn het met elkaar eens dat Europa er goed aan had gedaan bij het opstellen van de AVG te kijken naar handhavingsvoorbeelden van privacy volgens de Amerikaanse traditie.

In het Amerikaanse systeem worden privacyzaken tussen consumenten en bedrijven die producten en diensten aanbieden gehandhaafd door de Federal Trade Commisson (hierna FTC). Het ligt ook voor de hand om fricties ten aanzien van privacy binnen markt/consument kaders aan de orde te stellen. Vraagstukken met betrekking tot online-privacy worden aangepakt via misleidende of oneerlijke handelspraktijken. De FTC is al meer dan 100 jaar de handhavingsinstantie voor misleidende of oneerlijke handelspraktijken.
Bedrijven die zich niet aan privacyregels houden kunnen met de FTC 'consent agreements' sluiten. In deze consent agreements staan afspraken en verplichtingen waaraan bedrijven zich langdurig moeten houden. Bijvoorbeeld afspraken over verwerking van persoonsgegevens, afspraken over compliance en rapportage- en informatieverplichtingen.

Als een bedrijf zich niet houdt aan de consent agreements kan de FTC de federale Amerikaanse rechtbank verzoeken een boete op te leggen. In Europa biedt de richtlijn oneerlijke Handelspraktijken ook ruimte voor een dergelijke privacyhandhaving. Wanneer zou worden gekozen de Amerikaanse traditie als voorbeeld te nemen, zou er mogelijk effectiever gehandhaafde kunnen worden, sneller sancties opgelegd kunnen worden en meer focus op preventie en gedragsverandering bij bedrijven.

Jochem: Sinds Snowden is het bewustzijn rondom privacy bij bedrijven toegenomen. Er worden nieuwe producten ontwikkeld waarbij 'informed consent' het uitgangspunt is.
In een discussie met het publiek zegt Jochem dat Microsoft gelooft in het nut van anonieme data, en het belang ervan omdat er met behulp van deze data veel positieve toepassingen te bedenken zijn. Jochem benadrukt dat er een balans gezocht moet worden tussen het recht op privacy en de ruimte voor de ontwikkeling van slimme technologie.

Vanuit het publiek wordt de vraag gesteld of anonieme data wel echt bestaan? De-anonimiseren is immers mogelijk bij onvoldoende toezicht.
Ook het gebruik van G-mail door universiteiten en Hoge Scholen die gekoppeld zijn aan Surfnet wordt aan de orde gesteld. Nico: Er zou gekeken moeten worden naar het soort informatie wat er in cloud wordt opgeslagen bij het gebruik van een dienst. Gmail is wel te gebruiken voor alledaagse informatie maar niet voor gevoelige gegevens.

Jochem gaat kort in op de felle juridische strijd die Microsoft heeft gevoerd met het Amerikaanse Ministerie van Justitie. Amerika wilde e-mails van een verdachte in een drugszaak kunnen inzien. Deze e-mails zijn echter opgeslagen op servers in Ierland. In juli dit jaar heeft het Court of Appeals uitgesproken dat Microsoft de e-mails niet hoeft te verstrekken. De waarborgen van de Stored Communication Act gelden niet buiten de landgrenzen. Amerika kan zich niet op eigen wetgeving beroepen maar moet de weg van een internationaal proces volgen.

Stelling II:
Een lid van de werkgroep leidt de volgende stelling in door het bespreken van zijn ervaring als hoofd ICT –er van een zorginstelling die bij gevoelige jeugddossiers betrokken is. Zeker omdat er zoveel ketenpartners zijn in het traject van jeugdbescherming zijn er veel betrokkenen die toegang hebben tot gevoelige informatie (medische en strafrechtelijke data) over een kind en zijn ouders. Uitlekken van dit soort gevoelige informatie kan het kind en zijn toekomst beschadigen. Het kind zou ook recht hebben op 'the right to be forgotten'.

De stelling is wanneer het om gevoelige data gaat de overheid een infrastructuur moet garanderen die aan bepaalde normen moet voldoen, zoals privacy by design. Daarnaast moet de overheid actief helpen om deze infrastructuur uit te leggen. Het kennisniveau met betrekking tot privacy is erg laag of ontbreekt. Het zonder ondersteuning neerleggen van privacyvraagstukken als gevolg van de decentralisatie van zorgtaken bij gemeenten en hulpverleners is een te grote verantwoordelijkheid. Het zou goed zijn als de overheid rondom privacy een aantal standaardoplossingen voorschrijft die eventueel door marktpartijen verder kunnen worden uitgewerkt. De sprekers reageren op deze stelling vanuit een hun eigen invalshoek.

Jochem de Groot put uit zijn ervaring als beleidsadviseur internetvrijheid en mensenrechten bij het Ministerie van Buitenlandse Zaken. Van belang is volgens hem een heldere rubricering van alle data en een duidelijk beleid daarover. Het is noodzakelijk om een gelaagde structuur in te bouwen en bijvoorbeeld niet alle informatie als vertrouwelijk te rubriceren, zoals hij in de praktijk tegenkwam.

Vanuit het publiek komt de reactie dat een infrastructuur al wel bestaat maar nog wel moet worden verbeterd. Als voorbeeld wordt NORA genoemd (Nederlandse Overheid Referentie Architectuur): geeft voorwaarden rondom basisregistraties.

Nico van Eijk ondersteunt de stelling in het geval er zeer gevoelige informatie wordt verwerkt, zoals bij de jeugdzorg. Er is dan meer noodzaak om met een veilige infrastructuur te werken. Op decentraal niveau kan de kennis die nodig is voor een goede beveiliging niet verondersteld worden.

Romeo Kadir benadrukt dat de focus bij privacyproblemen erg ligt op de systemen, maar dat net zo belangrijk is de toename van privacy-bewustwording bij mensen zelf. Op dit moment is de mens een faalfactor als het gaat om privacy. Bij het verzamelen van grote hoeveelheden data zal men zich moeten afvragen of dit wel effectief is, anders ontbreekt de legitimatie ervan. We kunnen toch geen risicoloze samenleving bereiken. Systemen zijn in beginsel waardenloos, de mens is noodzakelijke voorwaarde voor waardenbewaking en waardenbescherming.

Stelling III
Een ander lid van de werkgroep stipt verschillende onderdelen van de Wet Computercriminaliteit III aan.
1. Het binnendringen van geautomatiseerde werken, 2. diefstal van data en 3. De hackbevoegdheid van de politie.
Vanwege de dreiging van terrorisme is de vraag hoe houden we Nederland veilig? Zijn deze instrumenten daarvoor echt noodzakelijk?

Zowel Nico van Eijk en Jochem de Groot zijn zeer kritisch over de *'extraterritoriale hackbevoegdheid'* in de Wet Computercriminaliteit III. Deze bevoegdheid maakt het mogelijk dat Nederland heimelijk kan binnendringen in een geautomatiseerd werk dat zich in het buitenland bevindt. Er wordt een opsporingsbevoegdheid toegepast op het territorium van een andere staat zonder diens hulp en medeweten. Dit staat op gespannen voet met het soevereiniteitsbeginsel. Landen die in elkaars systemen gaan binnendringen en eventueel informatie gaan aanpassen is een race naar de bodem.

Ook zijn de sprekers kritisch op het *'toezicht en het gebrek aan waarborgen'* in deze wet. De Centrale Toetsingscommissie zal toezien op de naleving van deze wet. Deze commissie bestaat echter uit politie en OM en voldoet daarom niet aan de scheiding der machten.

De balans ontbreekt in de Wet Computercriminaliteit III. De hackbevoegdheid van de politie is zeer ruim omschreven, namelijk alle geautomatiseerde werken. Om te hacken moet het gaan om een ernstig misdrijf waarvoor voorlopige hechtenis mogelijk is en dat een ernstige inbreuk op de rechtsorde vormt. Het ontoegankelijk maken of kopiëren van gegevens is toestaan bij een zeer ernstig misdrijf waarop een gevangenisstraf staat van 8 jaar of meer. De vraag is of de ernst en het ingezette middel wel in verhouding zijn met elkaar. De inbreuk op privacy wordt daarbij onderschat zeker omdat het Europese Hof van Justitie zich meermaals kritisch heeft uitgelaten over soortgelijke wet- en regelgeving.

Malware instaleren om bijvoorbeeld de toetsaanslagen van een verdachte te registeren. Bij welke partijen wordt deze gevaarlijke malware ingekocht? Wat als een app door toedoen van malware crasht? Ook bij deze politiebevoegdheid ontbreken duidelijke waarborgen, toezicht en checks en balances.

Nico van Eijk:
Concluderend: Deze wetgeving is slordig. Er is te weinig rekening gehouden met eerdere uitspraken van het Hof van Justitie en het Europees Hof van de Rechten van de Mens. Denk aan de uitspraak over de dataretentierichtlijn. Het accent daarin ligt op de proportionaliteit van de bewaarplicht. Het massaal verzamelen zelf wordt niet direct afgewezen maar er worden strenge eisen gesteld aan de onderbouwing van *de noodzaak en effectiviteit* van 'mass surveillance'. Er zitten bepalingen in de Wet Computercriminaliteit III die haaks staan op de jurisprudentie van de Europese hoven.
Ter onderbouwing van de noodzaak voor opsporing worden ook wel onjuiste uitspraken gedaan. Robert M werd ontmaskerd door de inzet van andere opsporingsbevoegdheden dan massale opslag van telecomdata.

Voortschrijdend inzicht over privacy
Jochem de Groot: Skype wil geen informatie over gevoerde gesprekken van gebruikers verstrekken aan de Belgische overheid. Volgens Skype is dit technisch onmogelijk omdat de gesprekken versleuteld zijn en Skype zelf ook geen toegang heeft tot de inhoud. Daarnaast is Skype van mening dat het niet onder de Belgische telecomwetgeving valt omdat het Europese hoofdkantoor in Luxemburg gevestigd is. Sinds 2013 zijn grote stappen gezet bij internetdiensten om te zorgen voor versleuteling van gesprekken. Dit is een wezenlijke keuzeverandering.

Big data en vertrouwen

Een recente ontwikkeling zijn de 'datagedreven polissen' die steeds meer verzekeraars aanbieden. Verzekeraars willen meer informatie waarmee zij risico's kunnen inschatten en de hoogte van de premie kunnen bepalen.

Denk bijvoorbeeld aan een apparaatje in de auto die het weggedrag van de gebruiker vastlegt. Met deze data kunnen er door verzekeraars profielen van mensen worden gemaakt.

Er moet een balans zijn tussen positief gebruik van big data en de vereiste bescherming van de privacy van gebruikers. Voorkomen moet worden dat op basis van deze profilering mensen worden gediscrimineerd of uitgesloten van een verzekering.

Toekomst

Tot slot wordt aan de panelleden gevraagd hoe zij de toekomst rondom privacy zien. Geen van de panelleden is negatief door het optimisme rondom voortschrijdend inzicht over privacy bij burger, ondernemingen en overheid.