# ICT en vertrouwelijkheid centraal bij tweede Innovatieplatform

**Is werken in de cloud veilig en hoe zit het met mijn privacy? Hoe zorg ik voor digitale geheimhouding van vertrouwelijke dossiers? Met deze en vele andere vragen kwamen bijna 200 advocaten op 1 december 2015 af op het tweede Innovatieplatform. De drukbezochte bijeenkomst in het West-Indisch Huis in Amsterdam stond dit keer in het teken van het thema 'ICT en vertrouwelijkheid'. Dagvoorzitter Roxane van Iperen leidde de discussies over privacy en digitale geheimhouding in goede banen.**

**DISCUSSIE 1: BESTAAT PRIVACY NOG?**
Deze vraag stond centraal in de eerste discussie, ingeleid door drie specialisten: Jeroen Koëter (Project Moore advocaten), Christiaan Alberdingk Thijm (Bureau Brandeis) en Rejo Zenger (Bits of Freedom).

***Rejo Zenger, Bits of Freedom:***
**"Kies voor dataopslag in Nederland, versleutel je e-mail en pas je wifi-gebruik aan"**

Zenger beet als eerste spreker het spits af en wees op het belang van vertrouwelijke communicatie tussen advocaat en cliënt op grond van het verschoningsrecht. Maar hoe vertrouwelijk is die communicatie nog in dit digitale tijdperk? Bijvoorbeeld op basis van alleen je telefoongegevens, die providers elk kwartier vastleggen en 6 maanden bewaren, is precies te achterhalen waar je bent geweest. Van gegevens die je in de cloud opslaat, weet je vaak niet waar die staan. De cloud is niets anders dan een computer van een provider, die in Nederland maar net zo goed in de Verenigde Staten kan staan. Maak je gebruik van een wifi-punt, is het heel goed mogelijk dat iemand anders digitaal over je schouders kan meekijken.

Het internet biedt volop mogelijkheden, maar het is ook noodzakelijk om jezelf op het wereldwijde web te beschermen. Allereerst door op de hoogte te zijn van er op dit gebied speelt in zowel Den Haag als Brussel, zoals de Wet computercriminaliteit en de digitalisering van de rechtspraak. Daarnaast is er volgens Zenger veel mogelijk om jezelf beter te beschermen. Kies bijvoorbeeld voor dataopslag in Nederland, versleutel je e-mail en pas je wifi-gebruik aan. Tip: gebruik de toolbox van Bits of Freedom!

***Christiaan Alberdingk Thijm, Bureau Brandeis:* "Er is een schrijnend gebrek aan handhaving"**

Volgens Christiaan Alberdingk Thijm is het recht op privacy springlevend. Kijk naar het activistische Hof in Luxemburg, soms meer wetgever dan rechter, die nationale wetgeving vernietigt. Alberdingk Thijm wees ook op het schrijnende gebrek aan handhaving en maakte de vergelijking met het milieu: het is wachten op ongelukken, we moeten er nu iets aan doen. Dat laatste geldt ook voor iedere individuele advocaat.

Op zijn vraag wie van de bijna 200 aanwezige advocaten beveiligde e-mail gebruikt, gaan slechts drie handen omhoog; een teken aan de wand. Aandacht voor digitale beveiliging is noodzakelijk, maar belangrijker is nog hoe je als persoon reageert op inbreuken op de privacy van jezelf en cliënten, aldus Alberdingk Thijm.

***Jeroen Koëter, Project Moore advocaten:***
***"*Combineer de voordelen van de cloud met voldoende aandacht voor vertrouwelijkheid*"***

Jeroen Koëter noemde het belang van privacy "actueler dan ooit". Advocaten kunnen niet zonder het recht op privacy, dat eisen cliënten ook. Het risico ligt bij advocaten zelf, daar moet de beroepsgroep zelf iets aan doen. Koëter heeft een "gezonde scepsis" ten opzichte van de cloud. De cloud is niet privacy-proof voor gevoelige cliëntgegevens. Weet goed wat je doet als gebruiker. Combineer de voordelen van de cloud met voldoende aandacht voor vertrouwelijkheid.

***Actualiteiten***
Na deze eerste drie inleidingen haakte dagvoorzitter Roxane van Iperen aan bij de actualiteit, zoals de discussie rondom het beschermen van data tegen overheidsdiensten.

Het Hof Den Haag heeft onlangs het afluisterverbod bekrachtigd. Geheime diensten mogen telefoongesprekken waaraan een advocaat deelneemt niet afluisteren zonder onafhankelijke toets die toeziet op de inzet van bijzondere bevoegdheden door de AIVD en MIVD. Een spectaculaire uitspraak, aldus Christiaan Alberdingk Thijm. Samen met de Verenigde Staten is Nederland het enige land zonder onafhankelijk toezicht. De uitspraak van het Hof is belangrijk om het recht gestalte te geven.

Een andere recente uitspraak is van het Europees Hof van Justitie, dat de regeling van de Europese Commissie voor doorgifte van data naar de Verenigde Staten (Safe Harbour-overeenkomst) onrechtmatig verklaarde. Eveneens met verstrekkende gevolgen, volgens Jeroen Koëter.

Aanvallen van hackers zijn aan de orde van de dag. Volgens Rejo Zenger is de techniek voorhanden om je hiertegen te beschermen. Bijvoorbeeld door je data in Nederland te houden, of door je e-mail te versleutelen. Mocht er sprake zijn van een datalek of een hack en komen je gegevens op straat te liggen, dan hebben die gegevens geen waarde.

Ook de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv) en de Wet computercriminaliteit kwam ter sprake. Belangrijk volgens Alberdingk Thijm is onafhankelijk toezicht, transparantie over wat je als overheid doet en voor wie, en dat gegevens niet langer worden bewaard dan nodig. Het is elke keer weer een afweging tussen de veiligheid aan de ene kant en gebruikersgemak aan de andere kant. Jeroen Koëter beaamde dit. Cloud-diensten als Dropbox zijn niet geschikt voor de advocatuur. Dat betekent niet dat je data helemaal niet in de cloud kunt opslaan, maar houd je inscriptiesleutels bij je zodat de provider er niets mee kan, luidde zijn advies.

***Discussie met de zaal***

1. *Is de hele privacy-discussie niet overtrokken? Beveiligen we een gemiddelde kruidenier niet alsof het een topjuwelier is?*
   Alberdingk Thijm: Nee, dat is niet overdreven. Onze beroepsgroep heeft een beroepsgeheim met een rechtstatelijke functie. Als advocaat heb je recht op privacy, maar heb je ook de plicht om je data te beschermen.
   Jeroen Koëter: Grote kantoren hanteren een ander veiligheidsniveau dan eenpitters.
   Rejo Zenger: Veiligheidseisen gelden voor alle advocaten. Gegevens van cliënten mogen nooit op straat komen te liggen.

2. *Komt de NOvA met richtlijnen over data en veiligheid?*
   Bart van Tongeren, per 1 januari 2016 de nieuwe algemeen deken van de Nederlandse orde van advocaten: Geheimhouding is het hoogste goed voor de advocatuur. Primair hebben advocaten een eigen verantwoordelijkheid om hun privacy en die van hun cliënten te waarborgen. Elk kantoor moet zelf uitmaken wat het gewenste veiligheidsniveau moet zijn. Tegelijk gaf hij aan dat de NOvA wel wil kijken of het mogelijk is een richtsnoer op te stellen voor data en veiligheid.
   Jeroen Koëter ziet een leidende rol voor de NOvA weggelegd, analoog aan Surfnet voor de academische wereld. Christiaan Alberdingk Thijm vindt dat de NOvA een zorgplicht heeft. Als eerste stap ziet hij het opstellen van protocollen.
   Rejo Zenger: Ongeacht wat de NOvA gaat doen of wat de wet zegt, heeft iedere advocaat een eigen verantwoordelijkheid.
   Uit de zaal: De Britse Orde heeft al richtlijnen, maak daar gebruik van.


3. *Wat zijn veilige alternatieven voor cloud-diensten als Dropbox, WeTransfer en Evernote?*
   Rejo Zenger: De techniek en producten veranderen voortdurend. Het gaat meer om de controle op je gegevens, Bijvoorbeeld door data in Nederland te laten hosten in plaats van in de Verenigde Staten, of door je communicatie te versleutelen.
   Rob Ameerun: een dubbele authenticatie (combinatie van wachtwoord en identifier) is het best.

**DISCUSSIE 2: DIGITALE GEHEIMHOUDING**

De tweede discussie voltrok zich rond het thema digitale geheimhouding, met als panelleden Rob Ameerun (Asfour), Wilbert Pijnenburg (Insite Security) en Jeroen Zweers (Kennedy Van der Laan).

***Jeroen Zweers, Kennedy Van der Laan:***
**"Ga bewust met je data om"**
De cloud is er en dat wordt alleen maar meer. Wees je daarom bewust van hoe je met data en databescherming omgaat. Vraag aan je provider waar je data staan opgeslagen (in Nederland of in de VS). Vraag ook naar hun certificeringen. Alleen voldoen aan de ISA-norm is overigens niet voldoende, dat is slechts de basis.

***Wilbert Pijnenburg, Insite Security:***
**"Digitaal rijbewijs voor de advocatuur"**
Pijnenburg pleitte voor een "digitaal rijbewijs voor de advocatuur", zodat advocaten weten hoe zij moeten omgaan met ICT en veiligheid in hun beroepspraktijk. Bijvoorbeeld als het gaat om het beveiligen van e-mail. Daarbij gaat het niet alleen om de techniek, het hoe. De basis is besef en begrip van waar je mee bezig bent.

***Rob Ameerun, Asfour:*** **"Lage 'sence of urgency'"**
De advocatuur loopt niet voorop in innovatie en databeveiliging, dat komt meer van cliënten. Een rapport uit de VS laat zien dat 80% van de advocatuur digitale veiligheid belangrijk vindt, maar dat slechts iets meer dan de helft hier iets aan doet. De 'sence of urgency' is dus laag. In de VS versleutelt 35% van de advocatuur zijn e-mail. In Nederland is dat 50% bij de grotere kantoren en minder dan 24% van de kleinere kantoren.

***Discussie met de zaal***

1. *Wat is de cloud?*
   Wilbert Pijnenburg: Dé cloud bestaat niet. Je provider slaat jouw gegevens ergens ter wereld op. De ene op servers in Nederland, de ander in de VS. Maar pas op: sommige Nederlandse providers besteden dit soms weer uit aan Amerikaanse providers zoals Amazon.com. Vraag dus altijd door waar de servers van je provider precies staan.

2. *Kun je e-mail in de cloud opslaan?*
   Rob Ameerun: Als je dat doet, doe het veilig en gebruik 'encrypted mail'.
   Jeroen Zweers: Bij Kennedy Van der Laan doen we dat voor sommige belangrijke dossiers

3. *Wanneer ben je als advocaat aansprakelijk?*
   Wilbert Pijnenburg: 100% aan alle regels voldoen haalt niemand. Een bepaald basisniveau van veiligheid is noodzakelijk. De vraag blijft alleen: welk niveau?

4. *Heeft de VS toegang tot mijn gegevens in de cloud?*
   Rob Ameerun: Er is steeds meer mogelijk. Maak daarom met leveranciers afspraken dat je data in Nederland blijven. Grotere kantoren hebben vaak een eigen server. Breng als kleiner kantoor je data onder bij een gespecialiseerde aanbieder.
   Wilbert Pijnenburg: Zorg er ook altijd voor dat je belangrijke data in de cloud versleutelt. Ga naar providers die jouw data in Nederland hosten.


5. *Moet ik mijn mail wel of niet versleutelen?*
   Wilbert Pijnenburg: Bedenk dat elke discussie met je cliënt gevoelige informatie kan bevatten, dus waak ervoor niet alles zomaar via onbeveiligde mail te versturen.
   Jeroen Zweers: Idealiter wel versleutelen, maar daarvoor is de techniek nog niet laagdrempelig genoeg. Er ontbreekt nog een standaard op dit gebied.
   Wilbert Pijnenburg: Het is nu inderdaad niet gebruikersvriendelijk. Er zou een digitaal certificaat moeten komen.
   Rob Ameerun: Als encrypted mail net zo gemakkelijk zou werken zoals diensten als Dropbox zou iedereen het al lang gebruiken.
   Jeroen Zweers: TLS biedt al de mogelijkheid om beveiligde mail te versturen op basis van een trust tussen twee servers. Daar merk je als gebruiker niets van.
   Wilbert Pijnenburg: Als je vanuit het buitenland mailt, gebruik dan niet zomaar de wifi van het hotel, maar leg eerst een beveiligde VPN-verbinding naar je eigen organisatie.

6. *Hoe zit het met Stork 3 en 4 in combinatie met de advocatenpas?*
   Elise Bravenboer, hoofd Financiën en Organisatie bij de NOvA en aanwezig in de zaal: Met Stork 3 kun je inloggen bij de Orde en de rechtspraak. Niveau 4 is om ook digitale handtekeningen te kunnen zetten.

*Het Innovatieplatform bestaat uit een serie bijeenkomsten waarbij advocaten en andere experts discussiëren over innovatieve ontwikkelingen die de advocatuur raken. Het eerste Innovatieplatform vond plaats op 13 oktober 2015, met als onderwerpen Alternative Business Structures en Mediation. Verder discussiëren naar aanleiding van het Innovatieplatform? Ga dan naar de NOvA-groep op LinkedIn.*