Verslag sessie 4 – Privacy & Encryptie

Bits of freedom is een stichting in Amsterdam; komt op voor fundamentele grondrechten op het gebied van digitale communicatie (bijv. we vechten ervoor dat de overheid niet zomaar gegevens kan aftappen en we zijn bezig met Facebook die gegevens van je bewaart).

Programma:

- Digitalisering van maatschappij in het algemeen
- Politiek
- Wat kunnen wij als advocaten zelf doen?

Rejo: wat voor telefoon hebben we? 1 iemand in de zaal heeft geen internet op de telefoon. Dat is goed, want het is belangrijk dat ons 'gedrag' wordt beschermd. In de huidige situatie waarbij veel dingen gedigitaliseerd zijn, je voortdurend wordt geregistreerd is het beginsel bescherming lastig te waarborgen.

Hoe lang worden gegevens bewaard over onze telefoongesprekken (niet de inhoud, wel het feit dat we de telefoongesprekken hebben gevoerd)?

Het goede antwoord; 6 maanden. Wet bewaarplicht & Communicatiegegevens zei voorheen een jaar; nu bewaren de providers de gegevens enkel voor administratieve doeleinden (facturatie). Dat zegt veel over ons sociale netwerk.

Uit de gegevens is af te leiden: de locatie van de telefoon. Als je regelmatig telefoontjes pleegt, wordt er een gedetailleerd beeld geschetst van je leven. Er wordt een overzicht gegeven van de verkeersgegevens die de provider bewaart met datum/tijd, soort gegeven (telefoongesprek/internetverbinding), postcode van plaats waar telefoontje wordt gepleegd/ verbinding werd gemaakt.

Er wordt een animatie getoond van een Duitser die laat zien waar de Duitser in een half jaar is geweest (Hannover, Berlijn etc.). Dit geeft een heel gedetailleerd beeld, zeker als het wordt gekoppeld aan publieke gegevens als Twitter. Zelf als de telefoon niet actief wordt gebruikt, kan er een goed beeld worden geschetst met welke personen je bent.

DUS: hoe zorg je ervoor dat je met iemand afspreekt, zonder dat het later herleidbaar is?

Zaal:

- Telefoon uitzetten
- Vliegtuigmodus
- Thuislaten
- Post: onze digitale communicatie kan met toestemming van de minister worden geopend. Envelop kan enkel worden geopend met toestemming van 'Den Haag'.

- Niet betalen met pinpas etc.

Doe je dit in Amsterdam, dan word je kenteken herkend. OV checkt in, checkt uit. Je wordt constant overal genoteerd en opgemerkt. Het is erg lastig met iemand in de hedendaagse maatschappij af te spreken zonder dat het later herleidbaar is. Spreek af midden op de Veluwe. De een gaat naar Arnhem, ander Nijmegen. Telefoon gaat in een kluis op het station. Dan loop je richting de heide of de duinen, zonder camera's. *MAAR: hoe maak je dan die afspraak?*

Hoe handig een telefoon ook is, het breekt in je privacy.

Politiek

Plasterk heeft een tijde geleden een wetsvoorstel ter consultatie aangeboden (wet op de inlichtingen en veiligheidsdiensten); hij zegt 'maak alsjeblieft commentaar op dit voorstel'. Voorstel: sleepnetbevoegdheid. AIVD mag nu telefoon aftappen indien ik word verdacht van een bepaald misdrijf. Als daar genoeg waarborg omheen zit, is daar niet heel veel mis mee. Indien Plasterk zijn zin krijgt, mag AIVD complete groepen van onverdachte mensen aftappen (ongericht aftappen); bijv. iedereen die naar Syrië belt. Ook wanneer er gewoon naar familie wordt gebeld. Dit is een heel brede manier van aftappen, wat verder gaat dan wat tot nu toe mocht. Door het sleepnet worden veel mensen afgetapt die niets onrechtmatigs hebben gedaan; dat is afwijking van een principe dat we kennen in Nederland.

Toezicht op de geheime diensten

Hoe zorgen we ervoor dat geheime diensten zich aan de wet houden? En hoe stoppen we hen indien ze onrechtmatig handelen? Toezicht is lastig, aangezien geheime diensten in het geheim werken. Er komt geen onafhankelijke rechterlijke toets aan te pas. Dat is problematisch. In het nieuwe voorstel staat 1 artikel, dat bizar is; het idee dat als er een tap wordt gezet, moet daarvoor toestemming worden gevraagd aan de minister. Om het toezicht te verbeteren, moet de CTIVD zo'n bevel erna beoordelen op rechtmatigheid. Het probleem is; als de CTIVD zegt 'tap is in strijd met de wet' dan gaat het bevel terug naar de minister. De minister mag dan zelfs zeggen 'we gaan het toch doen'. Als hij dat beslist, moet hij dat melden aan de CIVD. Zij hebben het laatste woord. Deze fractievoorzitters nemen een politieke beslissing; zij bepalen niet 'rechtmatig of onrechtmatig'.

Ander aspect van de wet

Delen van informatie met andere geheime diensten: geheime diensten opereren veel op give and takebasis. Heb jij informatie te bieden, geven zij jou ook informatie. Informatie uit tap kan straks ook gedeeld worden met NSA (Amerikaanse geheime diensten). Als Nederland geen informatie geeft aan NSA, geeft NSA ook geen informatie aan ons. Dit is vervelend; onze informatie komt in buitenlandse handen, die misschien anders met dit soort informatie omgaan.

Vonnis uit HR van vorige week, waarin minister Plasterk op z'n vingers wordt getikt

"Het is van groot belang dat degenen die tot een advocaat wenden, er op kunnen rekenen dat de vertrouwelijkheid van hun communicatie is gewaarborgd en dat slechts in bijzonder gevallen en onder toezicht van een onafhankelijk orgaan inbreuk kan worden gemaakt". Dus enkel en alleen als een onafhankelijke instantie (bijv. rechter) er iets van vindt, mag de inbreuk worden gemaakt. Big Brother Award won Plasterk vorige week, hij zei 'ik ben de eerste minister die gaat zorgen voor een onafhankelijke toetsing'. De realiteit is dat hij 2 dagen daarvoor door de rechter hiertoe gedwongen werd.

Wat nu?

Het wetsvoorstel heeft de minister teruggenomen. Hij heeft er veel commentaren op gehad (KPN zei 'dit is niet oké', maar ook gewoon burgers). Er is nooit een consultatie geweest waarbij de reacties zo groot waren. Dit voorstel gaat naar de Tweede Kamer, want de minister wil ermee doorgaan. Het is belangrijk dat advocaten helder maken aan de minister waarom dit niet oké is.

Deelnemer uit de zaal: wat is dan het probleem. Mijn cliënten en ik hebben helemaal niets te verbergen. Bij mij mogen ze gewoon informatie tappen. Rejo: ik denk dat je zo niet veel klanten meer overhoudt, elke klant heeft behoefte aan privacy. Guus Meeuwis luisterde altijd naar Raymond van het Groenewoud. Deze informatie wil hij eigenlijk voor zichzelf houden. Maar het komt op straat te liggen. Iedereen heeft iets te verbergen. De een is daar meer open in dan de ander.

Deelnemer uit de zaal: mensen komen erachter dat ik 24 uur per dag porno kijk. Dat is vervelend, maar de overheid kan hier niets mee. Rejo: enerzijds denk ik, ja ik kan me de reactie voorstellen, maar het gaat niet enkel om de overheid. Kijk wat er de laatste tijd is gebeurd qua datalekken. Bijv. profiel bij vreemdgangerswebsite. Op straat werd bekend dat ze een profiel hadden en ze hadden thuis iets uit te leggen.

Er wordt een vergelijking gemaakt naar de oorlog; De reden waarom in de gemeenteadministratie in brand is gestoken; dit is waardevolle informatie voor de Duitsers wordt vernietigd. Dat is nu niet meer mogelijk; alles is digitaal en overal naar boven te halen. Het maakt niet uit waar je in de wereld bent. De strijd die toen overzichtelijk was, is het al lang niet meer!

Deelnemer in de zaal: De mobiele telefoon is om ons leven te vergemakkelijken; we willen allemaal bereikbaar zijn, dus we zijn allemaal zichtbaar. Met de angst voor communicatiemiddelen komen we niet veel verder.

Rejo: hoe ga je hier als advocaat mee om?

Bijv. je krijgt veel mailtjes met Word, PDF. Het is makkelijk je als iemand voor te doen, je opent een PDF en je computer is besmet. Je kunt je hier makkelijk tegen wapenen: virusscanner, systemen up to date houden, back-ups maken bijvoorbeeld.

Binnen Bits Freedom wordt alles versleuteld. Op het moment dat de laptop wordt gestolen, kan niemand de inhoud van de e-mail achterhalen. Ook niet indien het wordt afgetapt. Als het bij een mailbox bij een provider staat, kan worden gezien met wie is gemaild, maar niet wat erin staat. De inhoud van je e-mails wordt beschermd.

Deelnemer in de zaal: die heeft dit wel eens geprobeerd. Ik kan dat wel doen, maar de klant moet dit programma dan ook hebben. Rejo: er zijn nu al advocaten die zeggen 'mij kun je bereiken door je mail te versleutelen', nu als je dat niet hebt, kan de andere kant dat nooit doen. Op het moment dat je het beschikbaar hebt, is er ruimte dat het wel kan. Als je denkt ik doe het niet, want de andere kant gebruikt het ook niet, dan verliest het z'n werking. Je moet je mail gewoon versleutelen, als advocaat heb je hier een verantwoordelijkheid in; je moet laten zien dat het belangrijk is dat je belangrijke informatie bij jezelf houdt. Niet dat heel de wereld hierbij kan.

Nog een vraag uit de zaal: heb je dan ook sleutelmail op je telefoon? Nee, de mensen met wie ik versleuteld mail, weten dat ik de versleutelde mail niet kan lezen als ik enkel mijn telefoon heb.

Nog een vraag: is de oplossing niet 'helemaal geen e-mail?' Rejo: de vraag is waartegen je je wil beschermen. Is dat een crimineel die een linkje stuurt, waardoor je een virus krijgt? Is dat de nationale politie, AIVD, NSA waartegen je je wil beschermen? Je moet dan kijken welke opties je hebt. En welke functionaliteit het nodig heeft.

The Cloud – documenten op een computer. Het is belangrijk je te realiseren waar je computer staat. Met dat in gedachte moet je je afvragen wie er toegang heeft tot het systeem. Het nadeel: de data staat in de VS. Bijv. Google kan er zelf doorheen lezen, maar ook dat niet meer zichtbaar is of Google de data verkoopt aan een andere partij. Sterker nog; je weet niet of de Nederlandse politie bevel geeft om in de gegevens te kijken. Rejo: Denk goed na over de consequenties!

Voor nu wil hij meegeven; the Cloud is een mooi systeem, maar er zitten nadelen aan en denk er over na.

Rejo: we hebben nu rechtszaken lopen tegen de nationale politie.

Vragen:

Grote bestanden, procesdossiers moet ik sturen naar advocaten. Zij zeggen ;wij kunnen niet ontvangen via outlook, dat mogen wij niet. ICT-concept heeft interpricedrive, dat is wel helemaal safe. Misschien moet je dan een portal creëren. Dropbox is ook niet veilig.

Rejo: alternatief is software die de functionaliteit van dropbox nabootsen, maar die je op je eigen server kunt draaien. Echter, dit systeem duurt wel lang om naar toe te werken. Je kunt hierdoor wel controleren wie bij de data kan. VPN: versleutelde verbinding tussen 2 plekken – niemand kan zien welke websites worden bezocht, welke bestanden worden gedownload etc.

Facebook is positief zegt een man uit de zaal. Het is gemakkelijk met mensen te communiceren. Rejo: ja er is meerwaarde, maar Facebook had privacyvriendelijker kunnen worden ingericht. Een sociaal netwerk kan ook op je modem thuis worden gezet. Dat is een andere opzet van het systeem; functionaliteit blijft het zelfde. Rejo: ik ben niet tegen social media, waar ik wel een probleem mee heb, zijn de keuzes over inrichting van het systeem.

Rejo: vaak wordt veiligheid tegenover privacy gezet. Ik denk niet dat dit waar is. Als je kijkt naar de politie – er is onderzoek gedaan naar wet naleving politiegegevens. Politiegegevens worden veel te lang bewaard! Geen Corps houdt zich meer aan de normen uit de wet. Bij de politie liggen heel gevoelige gegevens. Als die informatie te lang in een toegankelijk systeem blijft zitten, kan de informatie lekken. Ik denk dus 'het naleven van de WPG verhoogt bescherming van de informatie'.

Free Wi-Fi: ook gevaarlijk. Rejo: gebruikt nooit Wifi van de trein. Internetverbinding van de trein is makkelijk te volgen.

Zaal: er is wel een oplossing voor – de VPN.

Zaal: hoe zit het met het gebruik van Apps? Kun je dat ook terug zien? Rejo: nee.

Zaal: wat in het mapje zit dat je van de organisatie hebt gekregen = toolbox. Wat is dat?

Rejo: Hierin zitten tools waarbij je je eigen communicatie kunt beschermen. Als je nu een webpagina bezoekt, weet de website vanaf welk IP-adres je komt. Hij kan ook zien welke pagina's je opvraagt op de website. Er wordt in de Toolbox bijv. uitgelegd hoe je je harddisk kan versleutelen, welke andere chatapplicaties er bestaan naast Whatsapp, die je privacy beter waarborgen.

Rejo: je kunt makkelijk je harddisk versleutelen. TOR? Is een geavanceerd ding – het zorgt ervoor dat andere mensen niet kunnen onderscheppen & dat niet duidelijk is waar je vandaan komt.

Rejo: waartegen je je wil beschermen, bepaalt in welke mate je je gaat beschermen. Wat vind ik belangrijk? Er is geen zwart-wit antwoord. Je moet voor jezelf afwegingen maken.

Rejo: mensen die hier veel mee bezig zijn, hebben moeite met het bepalen waartegen je je moet beschermen. Maar in z'n algemeenheid kun je een aantal dingen overzien, bijv.

Wi-Fi is makkelijke bron voor hackers.

Wordt er veel misbruik gemaakt van informatie bij een advocatenkantoor?

Rejo: een Amerikaan had Gmail gebruikt, iemand wist google misbruikt en kon het wachtwoord genereren en kon de bestanden bij Apple gebruiken, doordat hij 'wachtwoord vergeten' had ingetypt en het naar de mail van Gmail had gestuurd (waar hij inmiddels in kon). Heel gevaarlijk!

In Nederland: er zijn heel veel datalekken bekend (kasboek.nl – hier kon je je kasboek bij te houden, die had iets fout gedaan en iedereens kasboek kon een jaar lang gezien worden). Het is bij een advocatenkantoor heel belangrijk dat er bescherming wordt gebonden.

Zaal: het is heel duur.

Rejo: als gegevens lekken, dan kun je je kantoor opdoeken – dit kost nog veel meer geld!

Voorbeeld aftappen van informatie.

Rejo: Valse zendmast door politie: I.p.v. dat je met KPN verbinding hebt, heb je met het busje verbinding. De politie kan daardoor bepalen waar een persoon is; ze mogen het niet, maar het wordt toch gedaan. Het is lastig omdat bij de politie een geheimhoudingscultuur geldt.

Vraag uit de zaal: de meneer is van de NOVA – Nederland is wereldkampioen afluisteren, stelt hij. Ook in absolute zin wordt er in Nederland meer getapt dan in heel de VS.

De meneer van de NOVA mist ‘de gebruiker’. Je kunt nog zo veel leuke beveiligingssystemen inlassen, de gebruiker speelt ook een rol. Heeft hij een beveiligingssysteem, maar typt hij in bij Google ‘Ik ben kees en ik woon in de Adelstraat’, dan maakt hij het anderen wel heel makkelijk zijn persoonlijke gegevens te verwerven.

Zaal: heb je een tip met betrekking op versleuteling van email op je smartphone.

Rejo: ik zelf heb veel mail, alle mail is versleuteld op mijn laptop. Op mijn telefoon wil ik mijn sleutel niet zetten. Als ik weg ben, kan ik de versleutelde mail niet lezen. Er zijn verschillende oplossingen je mail te versleutelen; makkelijke & moeilijke manieren. Kijk in de Toolbox!