Smartphones zijn een makkelijke prooi voor criminelen

WORDT U OOK AFGELUISTERD?

Iedereen met een mobieltje loopt risico zijn privacy kwijt te raken. Want mobiele telefonie biedt ongekende mogelijkheden voor zowel justitie als criminelen. De deskundigen, Martien Kuylman en Rob ten Hove, zijn het erover eens: ”Tappen, volgen, verdacht maken en informatie misbruiken, er is veel mogelijk.” TEKST KOEN SCHARRENBERG FOTO'S ANP EN ISTOCK

Rondom de mobiele telefonie hangt een zweem van geheimzinnigheid. We weten natuurlijk dat justitie onze gesprekken eenvoudig kan tappen en ook kan zien waar je bent geweest, afhankelijk van welke zendmast je telefoon heeft aangestraald. Die gegevens komen vaak terug in strafprocessen: het wordt gebracht als hard bewijs, onweerlegbaar. Maar dat is helemaal niet het geval. Heel weinig mensen weten wat er mogelijk en onmogelijk is op dit technologische gebied. 'Gewone' mensen niet en de meeste criminelen evenmin. Maar officieren van justitie, rechters en advocaten ook niet echt, blijkt uit onderzoek. Terwijl juist díe beroepsgroepen bepalen wie schuldig is aan een delict, achter de tralies moet verdwijnen, en voor hoelang. Dus: op grond van informatie die heel anders kan zijn dan het lijkt.

'Een rechercheur in je broekzak'

Martien Kuylman en Rob ten Hove weten wél precies wat de mogelijkheden en onmogelijkheden zijn van de moderne technologie. Zij zijn de grondleggers van het Nationaal Forensisch Onderzoeksbureau (NFO), een organisatie met een groot aantal deskundigen op diverse, forensische terreinen.
Martien Kuylman, ingenieur telecommunicatie, was hoofd van de afdeling onderzoek en ontwikkeling van de Amsterdamse politie en onder andere verantwoordelijk voor het systeemontwerp van het gsm-tapsysteem. Daarnaast was hij security manager bij grote telecombedrijven. Kuylman is tegenwoordig actief als adviseur en onderzoeker en wordt regelmatig gevraagd als getuige-deskundige in strafprocessen.
Rob ten Hove studeerde af in Forensic Sciences aan de Hogeschool Enschede, een relatief jonge studierichting die zich richt op de ontwikkelingen van het forensisch onderzoek. Op verschillende gebieden, van dna-problematiek tot de correcte interpretatie van digitale gegevens.
Beiden kijken uiterst kritisch naar het gebruik van mobiele telefoons en alle mythes die eromheen hangen. Plus: de manier waarop justitie er in sommige gevallen gebruik van maakt. Een gesprek waarin de beide onderzoekers elkaar aanvullen; Kuylman is vooral op technisch niveau de kenner, Ten Hove zorgt voor cijfers, aantallen en achtergronden. ”Wist je dat doorgewinterde criminelen een mobiele telefoon 'een rechercheur in je broekzak' noemen?”

Is via de telefoon communiceren dus per definitie onveilig?

”Kort door de bocht: ja. Het grootste misverstand dat leeft bij mensen, is dat je een telefoon in je handen hebt als je belt. Maar moderne mobieltjes zijn niets meer en niets minder dan computers, waarmee je 'toevallig' ook kunt telefoneren. Dus wat je met een computer uit kunt halen, kan ook met een mobieltje.”

Zoals?

”Ik, dus ook justitie – of een willekeurige deskundige – kan er heel simpel voor zorgen dat ik je af kan luisteren. Dat is wel een 'doemscenario', maar in theorie mogelijk. En het gaat verder: te weten komen wat je zegt als je belt en wat voor antwoord je krijgt, is het begin. Ook met wie je belt, door wie je »

WAT IS ER WAAR OF NIET WAAR

HET IS VEILIG OM...

■ Met een blackberry te 'pingen'.
"Een ping kan worden ingelezen door derden, met geavanceerde elektronica. Veiligheidshalve: niet waar dus."
NIET WAAR

■ De WhatsApp te gebruiken.
"Zeer eenvoudig te tappen." Ze gaan onversleuteld over de lijn: niet waar dus."
NIET WAAR

■ Te skypen.
"Is nu al gedeeltelijk af te luisteren. Vermoedelijk in de recente toekomst volledig. Niet waar. "
NIET WAAR

■ Te bellen met encryptie-software, zogenaamde 'versleutelde' boodschappen.
"Is een race met justitie. De nieuwste vormen, vaak gewoon te downloaden via internet, zijn 'veilig'. Zolang het duurt. Want niemand weet hoe snel de overheid er een achterdeurtje in open krijgt. Zie het maar als een bewapeningswedloop. Gedeeltelijk waar."
WAAR

■ Te bellen met een cryptophone.
"Er zijn hele goede cryptophones. Maar de ontvanger van de boodschap moet er dan ook een hebben. En je trekt er wel erg de aandacht van justitie mee. Gedeeltelijk waar."
WAAR

wordt gebeld, waar je bent, welke sms'jes je verstuurt en ontvangt, hoe laat en waarvandaan. Voor die gegevens moeten dan wel de juiste chips in je telefoon zitten.
Die kun je achteraf bekijken, maar ik kan er ook voor kiezen gewoon live mee te luisteren als je belt. En als je op internet gaat kan ik zien welke sites je bezoekt, letter voor letter volgen welke tekst je voor een mailtje intypt en naar wie je het verstuurt.
Ik kan zelfs op afstand een microfoontje aanzetten, zodat ik kan meeluisteren wat er gebeurt in de ruimte waar je mobieltje ligt. Dat kan dan weer niet 'zomaar': je kunt zulke 'bugs' alleen in een telefoon van iemand verstoppen als je er een tijdje over kunt beschikken. Vul zelf maar in hoe dat kan: een reparatie, telefoon die even 'kwijt' is of ergens moet worden afgegeven..."

Dat klinkt ingewikkeld en moeilijk realiseerbaar.
"Eigenlijk is het kinderlijk eenvoudig. Natuurlijk moet de man of vrouw aan de andere kant over een hoeveelheid specifieke kennis beschikken. Die is aanwezig bij justitie en politie, maar ook bij criminelen; in het Oostblok zitten bijvoorbeeld veel dubieuze 'deskundigen'. Helemaal kwetsbaar ben je als je met je mobieltje op internet zit. Je merkt er echt niets van dat je een handeling verricht die jou promoveert tot een makkelijke prooi voor criminelen. Klikken op de link van een website die je in de mail aangeraden wordt, kan al genoeg zijn. Of een foto openen die een vriend – of iemand die zijn mail gebruikt – je stuurt. Even kijken naar het 'leuke meisje dat jou zoekt', of toch even checken of jij echt die prijswinnaar bent, met de kans van één op 1 miljoen. Ook leuk: een blik werpen op die foto waarop jij – zogenaamd - bent gespot. Klik, en je hebt geen geheimen meer. Let wel, dat zijn de mogelijkheden die iedere computer heeft die verbonden is met het internet, dus op zich is dat voor zo'n Personal Digital Assistent (PDA) niet bijzonder; dat is eigenlijk een kleine computer."


Tussen afluisteraar en slachtoffer kunnen duizenden kilometers zitten.


Checken of het IMSI-nummer correspondeert met het IMEI-nummer.

Dus een mobieltje hoeft helemaal niet in andere handen te zijn geweest?
"Voor het plaatsen van een microfoontje wel, voor het afluisteren en volgen van iemands internet- en telefoonverkeer niet. Tussen de afluisteraar en het slachtoffer kunnen letterlijk duizenden kilometers zitten. De hele internetproblematiek gaat net zo op voor de gsm-telefonie."

Stel, ik gebruik geen internet op mijn mobieltje. Wordt het dan lastiger mij af te luisteren, te volgen etc.?
"Voor criminelen wel. Voor justitie blijft het *a piece of cake*, mits er sprake is van een gerechtelijk vooronderzoek. Helemaal in Nederland, dat afluisterland nummer 1 in de wereld is. In 2009 werden in Nederland bijna 25.000 telefoonnummers getapt, 86 procent mobiele telefoons en 14 procent vaste nummers. Ruim 2000 telefoons per dag. In de Verenigde Staten, met bijna twintig keer meer inwoners, worden per jaar zo'n 2000 taps geplaatst. Ons rechtssysteem is er helemaal op ingesteld informatie te verzamelen via afluisteren."

Daar is toch niks mis mee? Wie niets te verbergen heeft hoeft toch ook nergens bang voor te zijn?
"Dat zou mooi zijn als het waar was. In de praktijk werkt het alleen anders. De officier van justitie moet toestemming geven om iemand te tappen. Daar hoef je niet voor in een onderzoek te zitten, alleen een relatie hebben met iemand bij wie een gerechtelijk vooronderzoek loopt, dus 'verdacht' is, is al voldoende. Dat tappen breidt zich uit als een olievlek. Iedereen met wie zo'n 'verdachte' regelmatig contact heeft, kan ook worden getapt. Of het nou zijn voetbalteam is, het kerkkoor of criminele maatjes. Vervolgens wordt er een dossier aangemaakt, waarbij de rechterlijke macht uitgaat van de integriteit van de opsteller: het Openbaar Ministerie. De officier van justitie bepaalt namelijk welke informatie er in een dossier komt, wat op zich natuurlijk vreemd is. Hij gebruikt die info om de verdachte veroordeeld te krijgen. Nu zal vaak zo'n dossier naar eer en geweten worden opgesteld, maar het blijft mensenwerk. En helaas leert de geschiedenis dat er incidenteel sprake is van tunnelvisie: de verdachte moet worden gepakt, want hij is schuldig. En de ervaring leert dat je, door veel op zich onschuldige informatie aan elkaar te koppelen, heel goed een stevige verdenking van schuld kunt creëren."

Terug naar het tappen van een gsm-telefoon. Hoe gaat dat in zijn werk?
"Providers zijn in ons land verplicht aftappen mogelijk te maken. Het eigenlijke tappen gebeurt dus bij de provider. Die krijgt van de officier van justitie of de rechter-commissaris een nummer door met de opdracht: 'bewaar daar de gegevens van of laat ons meeluisteren.' Een 06-nummer staat niet op de simkaart van een telefoon, daar staat een zogenaamd International Mobile Subscriber Identity (IMSI)-nummer op. Pas bij de verkoop vindt een koppeling plaats tussen de simkaart (het IMSI-nummer dus) en het telefoonnummer. Die gegevens krijgt justitie en daar komt een tap op, in het 'eenvoudige' geval dat iemand de telefoon gewoon op zijn naam heeft staan. Elk telefoontoestel heeft ook een unieke registratie: het zogenaamde International Mobile Equipment Identity (IMEI)-nummer. Deze twee nummers, de IMSI en IMEI worden aan elkaar gekoppeld. Dus het omwisselen van een simkaart helpt niet tegen afluisteren."

En het gebruik van een prepaid toestel, anoniem gekocht in bijvoorbeeld een supermarkt?
"Als justitie je moet hebben, kunnen ze je binnen een paar minuten tappen. In ons land rijden namelijk zo'n twintig zogenaamde 'IMSI-catchers' rond. In de buurt van een 'verdachte' vangen ze daarmee alle telefoongesprekken op. Op de opgevangen IMSI's kunnen taps worden gezet. Ook kunnen, wanneer de persoon zich verplaatst, opnieuw de IMSI's bekeken worden en gezocht worden naar een 'match'. Probleem is dat die IMSI-catchers storingen bij het andere mobiele verkeer veroorzaken. Maar dat merkt vrijwel niemand."

Dan straal je vervolgens met je telefoon een bepaalde mast aan en vervolgens weet justitie precies waar je bent?
"Zo laten ze het vaak voorkomen, maar het is niet waar. Op het platteland kan de dekkingswijdte, zeg maar de cirkel waarbinnen je een mast aanstraalt, zo'n 30 kilometer zijn. In de steden met al zijn masten, is het een paar honderd meter. Ideaal dus om iemand op een plaats delict te plaatsen, zou je zeggen. Het OM gebruikt die gegevens dan ook graag en vaak. Maar ook regelmatig onjuist en onvolledig. Want elk mastnummer bestrijkt slechts een gedeelte van de cirkel, meestal 120 graden. De cirkel is dus verdeeld in drie even grote delen, sectoren van 120 graden elk. Dus je kunt die drie sectoren bijvoorbeeld A, B en C noemen. Zo'n sector wordt door een soort omgekeerde bloembak »

'Ik kan zelfs op afstand een microfoontje aanzetten zodat ik kan meeluisteren'

GOED BOEK

VERBRIJZELD

Als er een afgeknipt teentje met een formidabele losgeldeis wordt opgestuurd naar het grootste roddelblad van Aberdeen, staan stad en land op stelten. De Aberdeense politie lijkt niet opgewassen tegen de uiterst efficiënt opererende ontvoerders. TEKST GER LAAN

WAAR GAAT VERBRIJZELD OVER?

Alison en Jenny McGregor zijn een zingend moeder-dochter-duo, gelanceerd via de talentenrace *Britains Next Big Star*. Het duo wordt ontvoerd. Binnen twee weken moeten fans een losgeld van ettelijke miljoenen inzamelen. Om hun losgeldeisen kracht bij te zetten, sturen de kidnappers een afgeknipte kleine teen op. Brigadier Logan McRae en zijn collega's proberen met alle macht de twee te vinden, maar de kidnappers hebben geen enkel spoor achtergelaten.

Hoofdrolspeler Logan McRae maakt in dit zevende deel van de *Cold Granite*-reeks zowaar promotie. Omdat hij als enige de link legt naar de ontvoerders, wordt hij gepromoveerd tot inspecteur. Maar dat weegt niet op tegen de brandstichting in zijn huis waarbij zijn vriendin Samantha zwaar gewond raakt.

WIE IS STUART MACBRIDE?

De schrijver woont en werkt in Aberdeen (Schotland), studeerde architectuur in Edinburgh en debuteerde in 2005 met *Steenkoud (Cold Granite)*.

TITEL: ***Verbrijzeld (Shatter the Bones)***
AUTEUR: **Stuart MacBride**
PAGINA'S: **413**
UITGEVER: **Unieboek**
PRIJS: **€ 18,99**

CIJFER **8+**

Je bent helemaal kwetsbaar als je met je mobieltje op internet zit.

bestreken. Kijk maar eens omhoog hoe een zendmast eruitziet, dan zie je de structuur. Justitie zegt dan: De telefoon van de verdachte straalde zendmast nummer 100 aan, dus hij was vlak bij de plek van de moord, of de overval, noem maar op.

Maar als hij sector 100 C aanstraalde, kan dat ook zijn alibi zijn, bijvoorbeeld als de moord is gepleegd in het gebied van sector 100 A. Dat kan een hele andere straat zijn.

Alleen vermeldt justitie de sector nooit. Daar komt nog bij, dat een telefoon altijd het beste, dus sterkste signaal kiest. Een verdachte kan bij wijze van spreken 100 A hebben aangestraald, waar de moord is gepleegd, maar daar niet zijn geweest.

Dan stond hij een stuk verderop, maar stond er bijvoorbeeld een groot gebouw tussen zijn telefoon en de mast die hij eigenlijk normaalgesproken aan zou stralen, laten we zeggen mast 200. Dan kiest de telefoon voor een makkelijker en beter signaal (100 A dus) en is hij opeens wél verdachte.

Wij adviseren dan ook vaak advocaten, om ter plekke door ons een meting uit te laten voeren. Dat heeft al tot opvallende resultaten voor de verdediging geleid."

"Kijk," zegt Martien Kuylman ter afsluiting, "dit mobieltje biedt nog de meeste privacy." Hij pakt een mobiel, model koelkast en minstens tien jaar oud. "Maar toch ook heel gemakkelijk af te luisteren en te volgen. Er is maar één advies voor iedereen die vertrouwelijke informatie uit wil wisselen: niet mailen en al helemaal niet bellen. Terug naar de handgeschreven brief en dichtgeplakte envelop..." «

VERDUISTERING VIA DE TELEFOON

Vanuit een hotel in Rotterdam wordt gebeld naar een bank en, volgens het OM, vervolgens geld verduisterd. Een verdachte belt rond dat tijdstip met een mobiele telefoon en straalt daarbij mast 38 aan, vlak bij het hotel. Het OM stelt: hij zat in het hotel en is dus medepleger. Nader onderzoek door de verdediging toont echter aan, dat mast 38 vrijwel geen bereik heeft in het hotel en dat er maar liefst twee masten zijn die een beter bereik hebben. Met andere woorden: de verdachte was gewoon niet in het hotel en wordt vrijgesproken.