

Privacy internetgebruiker onder druk

Op aanbeveling van de Commissie Mevis werd op 1 september 2004 de Wet Vorderen Gegevens Telecom aangenomen. Later zijn nog meer privacygevoelige wetten gevolgd. Op grond van een van die wetten zag het overheidsinstituut CIOT het licht. De bevoegdheden van het CIOT en wijze waarop van het CIOT gebruik wordt gemaakt, zetten de privacy van internetgebruikers verder onder druk.

Het CIOT, Centraal Informatiepunt Onderzoek van Telecommunicatie, ontvangt iedere dag van ISP's of hosting providers een kopie van relevante klantgegevens. Uit artikel 4 lid 2 van het besluit bij de Wet Vorderen Gegevens Telecom blijkt dat het om de NAW-gegevens van internetgebruikers gaat, hun telecom-pakketten en hun telefoonnummers. De politie en justitie kunnen die gegevens inzien.

De door het CIOT verkregen informatie wordt ca. 3 miljoen keer per jaar opgevraagd door politie, FIOD of AIVD, oftewel een dikke 8.000 keer per dag. Dat heeft *Bits of Freedom* uitgezocht. BoF is een organisatie die op de barricades staat ter verdediging van de internetprivacy en online communicatievrijheid.



Afgezien van het feit dat de Wet Vorderen Gegevens Telecom een onbehaaglijk gevoel oproept – ik bedoel: wat gaat het iemand ene moer aan wat mijn NAW-gegevens zijn als ik zit te surfen! -, zijn de laagdrempelige procedure voor politie en justitie om die informatie op te vragen en het gebrek aan controle op het CIOT buitengewoon zorgwekkend. In ieder geval als het om de bescherming van privacy van internetgebruikers gaat. Hoewel de uitvoering van de wet met enige zorgvuldigheidsvereisten is omkleed, is het tot op heden onduidelijk of en in hoeverre aan die vereisten daadwerkelijk uitvoering wordt gegeven.

Correcte uitvoering van de opvraagprocedure vergt dat alle verzoeken bij het CIOT worden gecontroleerd. Inhoudelijke toetsing

betekent zijn er voldoende gronden voor de opvraging, is de verzoeker bevoegd, zijn bewaring en vernietiging van de verkregen gegevens verzekerd. M.a.w. gaan de gegevens die niet relevant blijken te zijn, wel degelijk door de versnipperaar en niet als propje in het papieremmertje. Maar, niet is duidelijk wie dat controleert en of een dergelijke controle überhaupt telkens bij iedere bevraging plaatsvindt. Sowieso is er onvoldoende documentatie van de interne processen bij het CIOT, althans niet iets dat kennelijk op basis van de Wet Openbaarheid Bestuur op tafel kan komen. Het is dus evenmin controleerbaar of de verzoeken bij het CIOT met voldoende rechtsgrond en bevoegdheid plaatsvinden.

En dan is er nog de wet Bewaarplicht Telecommunicatiegegevens die in juli 2009 in werking is getreden. Op grond van die wet zijn de Wet Economische Delicten (WED) en de Telecommunicatiewet (Tcw) aangepast.

In de telecommunicatiewet stond overigens al dat ISP's hun netwerk geschikt moeten maken voor tappen door politie en veiligheidsdiensten. In 2008 waren dat ongeveer 2000 taps per dag. Ook moeten de ISP's meewerken aan aftapbevelen. Aftapbevelen zijn

onderworpen aan rechterlijke controle. De rechter-commissaris geeft de Officier van Justitie de toestemming om te tappen, maar de R-C verleent de taptoestemming na summere toetsing van de gronden en feiten die de OvJ zélf aanreikt.

Daar is dus nu ook de Wet Bewaarplicht Telecommunicatiegegevens bijgekomen, de implementatie van de zgn. Europese Dataretentierichtlijn. ISP's moeten op grond van die wet verkeers- en locatiegegevens, e-mailberichten en internettelefonieverkeer (dus VOIP-calls) plus de daarbij behorende identificatiegegevens voor de duur van 12 maanden bewaren. Dat betekent dat de ISP en de overheid, waarschijnlijk nog beter dan uzelf weten wie er op 325 dagen geleden u heeft gemaïld of geskyped en welke sites u die dag heeft bezocht. Die gegevens dienen op bevel van de R-C aan politie en justitie te worden vrijgegeven in het kader van onderzoeken, opsporen en vervolgen van ernstige misdrijven, aldus 13.2a lid 2 Tcw.

De informatievergarende overheid heeft zich een wettelijk kader aan te trekken, dat *lijkt* te rijmen met artikel 8 Europees Verdrag voor de Rechten van de Mens (EVRM). In dat artikel, meer bepaald het tweede lid, staat dat geen inmenging van enig openbaar gezag is toegestaan op het privacyrecht van individuen, tenzij een dergelijke inmenging bij de wet is voorzien en *noodzakelijk* is in het belang van a) nationale veiligheid, b) de openbare veiligheid of c) het economische welzijn van het land, d) het voorkomen van wanordelijkheden en strafbare feiten of e) de bescherming van – kortweg- de vrijheid van anderen. Er moet dus een wettelijke grondslag zijn om van overheidswege inbreuk te maken op de privacy van haar onderdanen en de inbreuk moet noodzakelijk zijn om een beperkt aantal welomschreven doelen te kunnen bereiken.

De inbreuk op de privacy van niet-verdachten is volgens justitie noodzakelijk omdat de uitbreiding tot niet-verdachten kan bijdragen aan de opsporing van strafbare feiten. Het is onzeker of met dat argument voldaan is aan de motiveringseis van het EVRM. Ik zie namelijk de noodzaak van een dergelijke uitbreiding niet in.

Volgens de wetgever is het opvragen van verkeersgegevens voor de opsporing van belang om zicht te kunnen verkrijgen op het telecommunicatiegedrag en het patroon van contacten van een persoon. Blijft evenwel onduidelijk of dit belang groot genoeg is om de privacy inbreuk te rechtvaardigen. De wetgever gaat ervan uit dat de bestaande bevoegdheden verenigbaar zijn met het EVRM.

Online bedrijven halen vergelijkbare capriolen uit om zoveel mogelijk informatie over hun internetbezoekers te verkrijgen. De meeste gegevens worden achtergelaten via zgn. webbugs. Dat zijn 1 px-plaatjes of 1px-images die het surfgedrag registreren. Zo worden via webbugs geregistreerd: het browsertype, het bezochte webadres, duur van het bezoek, welke handelingen op die webpagina zijn verricht, de webpagina waar de bezoeker vervolgens naartoe klikt en zijn of haar IP-adres. Het is nu juist de registratie van het IP-adres dat maakt dat inbreuk wordt gemaakt op privacy. Het zal de internetbezoeker immers niet ontgaan dat daar waar hij zich eerder zat te struinen op online aanbiedingen voor een appartementje aan de Costa del Sol, hij even later op een andere webpagina in de zijkant reclamebanner zover residenties aan de Costa's ziet verschijnen. Het is gek, maar doorgaans wordt minder zwaar aan de privacy-inbreuk door bedrijven getild dan aan die gepleegd door de overheid. Een reden kan zijn dat de overheid op grond van de – al dan niet correct(e) - vergaarde kennis de sterke arm kan inzetten. Tegen dat machtsmonopolie staat de burger machteloos.

28 september 2010, mr. F.J. Van Eeckhoutte, ICT/IE & Corporate,
www.vaneeckhoutteadvocaten.nl