HC 6, 13-03-2018, IT & Strafvordering (II)

Grondslag datamining
Dit is in de fase vóór opsporing (internetsurveillance) Maar geeft art. 3 PW 2012 voldoende grondslag? Het antwoord is nee, want er wordt op systematische wijze veel informatie ontvangen van mogelijk van onverdachte personen. Maar zit er ook een verschil tussen vergaren en bewaren? Het binnenhalen van veel informatie, ook van eventueel onverdachte personen, is geen probleem. De nadruk ligt op de fase daarna, namelijk het bewaren en de gegevensbescherming. De Wet politiegegevens geeft invulling aan de bescherming van deze informationele privacy, maar er wordt weinig waarde gehecht aan deze privacy in het kader van verzameling van persoonsgegevens.

Als je kijkt naar de wetsgeschiedenis van Wet Computercriminaliteit II, dan vind je een vergelijkbare benadering met betrekking tot de internetsurveillance en over de toelaatbaarheid. De bevoegdheid om rond te kijken op het internet impliceert niet de bevoegdheid om stelselmatig gegevens van onverdachte personen 'zo maar' te downloaden. Deze gegevens mogen alleen worden opgeslagen als ze **noodzakelijk** zijn voor de politietaak. Voor de opsporing van een bepaald strafbaar feit geldt dat gegevens downloaden, opslaan, analyseren en verbanden hiertussen zoeken kennelijk noodzakelijk is. Dat is dan ook toegestaan.

In art. 3 lid 1 Wet Politiegegevens is die noodzakelijkheid verankerd in de wet. Uit de wetsgeschiedenis van dit artikel blijkt dat er van de politie wordt verwacht de gegevens rondom het strafbare feit verzamelt, verwerkt en in verband brengt. Het zal vaak gaan om personen waartegen (nog) geen verdenking bestaat. De gelegde verbanden en opvallende feiten die naar voren komen, kunnen aanleiding zijn tot verdieping en gerichte verwerking van een bepaald doel.

Het perspectief van het EHRM is ook belangrijk. Het arrest Rotaru vs. Roemenië is dan zeer verhelderend. Hieruit blijkt dat ook art. 8 EVRM (recht op privacy) aan het licht komt als openbare gegevens systematisch worden opgedaan en worden opgeslagen. Evenals het arrest PG vs. United Kingdom, waarin de redelijke verwachting van privacy duidelijk naar voren komt. Privé-dingen kunnen ontstaan zodra een systematische of permanente registratie van bepaald materiaal uit het publieke domein ontstaat. Dit is de reden dat de bestanden van een bepaald individu, die verzameld zijn door beveiligingsdiensten, binnen het kader van art. 8 EVRM vallen. Ook wanneer de informatie niet is verzameld door een verborgen of exclusieve methode. De nadruk ligt dus steeds op de privacyaspecten van 'bewaren'.

De grondslag van dataverzameling (art. 3 PW) is mogelijk geen probleem. Het verzamelen op zich is geen directe inbreuk op klassieke kernwaarden van privacy (mits er geen binnendringende technieken worden gebruikt). De Wet Politiegegevens vormt een voldoende kader voor gegevensbescherming met de regels omtrent bewaarduur, inzagerecht, verstrekkingen etc. Maar de hoeveelheid gegevens kan een probleem zijn, tenzij het niet bovenmatig en alleen noodzakelijk wordt gebruikt.

Drones
In het arrest **De Raven** wordt de verdachte vervolgd voor wietteelt en diefstal van elektriciteit. De verdachte komt met het verweer dat de inzet van een drone zonder wettelijke grondslag is geschied, terwijl dit wel een inbreuk op persoonlijke levenssfeer van burgers veroorzaakt. Dit zou moeten leiden tot vormverzuim en bewijsuitsluiting. Het Hof oordeelt dat er geen specifieke wettelijke grondslag hoeft te zijn voor de inzet van een drone. De inzet van drones kan op verschillende manieren namelijk geschieden: met of zonder beeld- of warmtecamera, kort- of langdurig en wel of niet gericht op een bepaald object of persoon. Het Hof stelt vast dat de inzet van 'De Raven' met toestemming van college van P-G is geschied en dat bij de inzet een camera is gebruikt waarmee geen personen zijn te identificeren. De drone heeft opnames gemaakt van wijken in Arnhem en niet van een specifiek object. Bij verdachte is een opvallende warmte-uitstraling van zijn woning geconstateerd, dit is volgens het Hof niet het onrechtmatig inzetten van een opsporingsmiddel. Art. 3 PW 2012 en 141 Sv volstaan in casu.

Onderzoek 'gegevensdragers' (computers en smartphones)

Er is in de rechtspraak verschil in opvatting over de toelaatbarheid van het verrichten van onderzoek in smartphones. Dit is in het kader van inbeslagneming van voorwerpen ter waarheidsvinding. Art. 134 Sv gaat over wat inbeslagneming precies is. Art. 94 Sv over de beslaggronden en doelen ervan. Art. 95 Sv e.v. gaan over de beslagbevoegdheden. Het gaat voornamelijk over situaties waarin de politie (bijvoorbeeld bij een aanhouding) een smartphone in beslag neemt en onderzoekt.

In het arrest **Onderzoek Smartphone** is het uitgangspunt van de HR dat voor waarheidsvinding onderzoek mag worden gedaan aan inbeslaggenomen voorwerpen voor het strafrechtelijke onderzoek. Gegevens die zijn opgeslagen in computers zijn daar geen uitzondering op. Maar geldt dit uitgangspunt tegenwoordig nog wel voor een 'computer' zoals de smartphone?

Het Hof Arnhem-Leeuwarden stelt dat art. 94 Sv te weinig specifiek is bij de inbeslagname, onderzoek en gegevens uitlichten van een smartphone en een ontoereikende grondslag heeft in het licht van art. 8 EVRM. Het is dan vereist dat een hogere autoriteit betrokken is. Hiertegenover staat de uitspraak van het Hof Amsterdam waarin wordt beslist dat het wel voldoende grondslag is. Het onderzoek is steeds toetsbaar aan de proportionaliteit en subsidiariteit in het licht van de verdenking.

Niet alleen art. 94 Sv dient als grondslag, maar vooral art. 95 Sv. Het gaat om een onderzoek aan inbeslaggenomen voorwerpen en art. 95 e.v. bieden nadere normeringen en waarborgen. Maar is er dan een steeds hogere autoriteit vereist? Dit is bij de fase 'beslag' erg onpraktisch, daarnaast ontbreekt die bemoeienis van de hogere autoriteit. Bij 'search & seizure' die de privacy kan raken, zodanige waarborgen komen dat willekeur zoveel mogelijk wordt voorkomen (EHRM). De voorkeur van het EHRM gaat uit naar toetsing vooraf door een onafhankelijke autoriteit, maar bij ontbreken of gebrekkigheid van de toets is compensatie achteraf mogelijk. Het Nederlandse recht biedt achteraf voldoende mogelijkheden, zoals de mogelijkheid tot beklag over inbeslagneming (art. 552a Sv).

Er zijn twee benaderingen: de begrenzing van de bestaande bevoegdheid van de opsporingsambtenaar in concreto (proportionaliteit en subsidiariteit); er is een mogelijk ernstig inbreuk op de privacy (onvoldoende waarborgen).

Stelselmatige inwinnen van informatie
In het arrest **Undercover op Facebook** wordt de verdachte vervolgd wegens deelneming aan een criminele organisatie. De politie heeft een nepaccount aangemaakt (op Facebook) en met verdachte contact gezocht met het doel om informatie te verkrijgen. Via het nepaccount worden berichten en foto's gepost en vriendschap verzoeken verstuurd. Er werden regelmatig kopieën gemaakt van de pagina van verdachte. De rechtbank kijkt of er inbreuk op het privacyrecht is en welke mate die inbreuk heeft. Dit is analoog aan stelselmatige observatie (art. 126g Sv): wel of niet beperkte mate van inbreuk scharniert rond stelselmatigheid inzet methode: duur; intensiteit; plaats; doel; wijze waarop; graad van verdenking. Is de methode geschikt om een min of meer compleet beeld te krijgen van bepaalde aspecten van iemands privéleven? Als de observatie stelselmatig is, dan is er een specifieke grondslag vereist met nadere normering, anders volstaat art. 141 Sv.

Hier speelt het stelselmatig inwinnen van informatie (art. 126j Sv). De wetgever heeft bepaald dat het deelnemen aan een internet-discussieforum hieronder ook kan vallen. In het algemeen is heimelijk aanwezig zijn rondom verdachte. De rechtbank oordeelt dat er sprake is van stelselmatigheid omdat er regelmatig data wordt opgeslagen, maar er is niet aan de formaliteiten van art. 126j Sv voldaan.

Decryptiebevel
Een andere bevoegdheid is de doorzoeking ter vastlegging van gegevens (art. 125i Sv). Het gaat hier om doorzoeking van een plaats, zoals woning/ kantoor/ auto, met als doel het vastleggen van gegevens die op die plaats op een gegevensdrager zijn vastgelegd/opgeslagen. Dit kan een geautomatiseerd werk zijn, maar ook een papieren dagboek. Art. 125j Sv is een uitbreiding van de bevoegdheid. In dit artikel wordt bepaald dat bij een doorzoeking in elders aanwezige computers mag worden gezocht voor zover van personen die op de plaats van doorzoeking werken, toegang hebben tot die computers.

VB: FBI vs. Apple. iPhone 5C van een verdachte is in beslag genomen in zaak met veel doden en gewonden. De gegevens waren echter versleuteld en de FBI wilde dat Apple een software ging ontwikkelen zodat onbeperkt wachtwoorden kunnen worden uitgeprobeerd. Voorwaarden die in jurisprudentie zijn ontwikkeld zijn:

- Subsidiariteit: alleen als er geen specifieke grond is, waarmee hetzelfde bereikt kan worden
- De derde dient een zeker verband te hebben met de zaak
- Alleen in uitzonderlijke omstandigheden toepasbaar
- Niet onredelijk belastend zijn voor de derde

FBI kreeg de court orde, maar Apple verleende geen medewerking. Uiteindelijk is de zaak teruggetrokken want een andere partij bood de FBI hulp en de telefoon leverde niets op. Dit is vergelijkbaar met ons decryptiebevel aan derden.

Het uitgangspunt in de VS is dat alles mag, mits het niet in strijd is met de wet. Er mag geen decryptiebevel worden gegeven aan de verdachte vanwege het verbod van zelfincriminatie (nemo tenetur). Als justitie zeker weet (uit andere bron) dat het gaat om incriminerend materiaal, dan is het geen probleem, maar anders is er immuniteit voor de verdachten.

In Nederland is in art. 125k lid 3 Sv bepaald dat het decryptiebevel niet aan verdachte mag worden gegeven. Dit hangt samen met het nemo tenetur-beginsel van art. 6 EVRM. In Wet Computercriminaliteit III is het voorstel om een bevel tot decryptie aan verdachte mogelijk te maken bij verdenking van art. 240 Sr (kinderpornografie) en terrorisme. Het voldoet niet aan de nieuwe strafbepaling (art. 184 Sr) en het voorstel is geschrapt. Het komt dus niet in Wet Computercriminaliteit III. De kern van de discussie of er wel of geen decryptiebevel aan verdachte kan worden opgelegd is of het wel of niet in strijd is met het nemo tenetur-beginsel. Het EHRM stelt dat het aan het OM is om bewijsmateriaal te verzamelen zonder dwang tot bekentenis of verklaringen. Het nemo tenetur-beginsel strekt zich niet tot het materiaal dat onafhankelijk van de wil van de betrokkene bestaat.

VB: in Jalloh werd tegen de wil van een verdachte een braakmiddel toegediend om bolletjes drugs te verkrijgen, dit was in strijd met art. 6 jo. 3 EVRM. De wijze van verkrijging komt meer centraal te staan. De vier ijkpunten in Jalloh:

- De aard en mate van dwang
- Het gewicht van het publiek belang in de opsporing en vervolging van het strafbare feit in casu
- De aanwezigheid van relevante waarborgen in de procedure
- De manier waarop het afgedwongen materiaal wordt gebruikt

Ook al bestaat het materiaal onafhankelijk van de wil van de verdachte, dan kan het nemo tenetur-beginsel alsnog worden geschaad. Als het materiaal niet onafhankelijk van de wil kan worden verkregen. Er is een actievere medewerking van verdachte nodig. Dit toegepast op het decryptiebevel geldt dat het wachtwoord in het hoofd van de verdachte zit en daarom bestaat onafhankelijk van de wil van verdachte.

Terughacken (CC III)

In Wet Computercriminaliteit III is de bevoegdheid tot heimelijk binnendringen van een computer, in gebruik of mede in gebruik bij verdachte in het voorstel opgenomen. In de volksmond wordt dit terughacken genoemd. Met de inzet van de bevoegdheid kan de toegangsbeveiliging worden doorbroken en mag er spyware worden geïnstalleerd. De bevoegdheid kent twee stappen: het binnendringen en doelgebonden onderzoekshandelingen verrichten.

Dit kan zijn het achterhalen van sleutels via logging software, aangekoppelde USB-sticks, externe harde schijf om gegevens vast te leggen, maar nu ook heimelijk. Bijvoorbeeld het aanzetten van een webcam of microfoon om gesprekken af te luisteren of ter observatie.

De bevoegdheid komt 3x in de wet, waarbij het kan worden ingezet na diverse typen verdenkingen. De toegevoegde waarde van de bevoegdheid schuilt in de heimelijkheid van de toepassing. Het mag alleen worden ingezet op bevel van de OvJ, nadat R-C een machtiging heeft verleend. Het is beperkt in duur (max 4 weken), maar dit kan steeds verlengd worden. Er is dan wel telkens een nieuwe afweging. De toegang tot de computer mag worden bewerkstelligd door middel van bekende ‘programmeerfouten’.

De politie mag zelf ontdekte slechte beveiliging tegen binnendringen dus onder de pet houden (art. 126ffa Sv).