Gerechtshof Arnhem-Leeuwarden, 22 april 2015, ECLI:NL:GHARL:2015:2954, *Computerrecht* 2015/127, m. nt. J.J. Oerlemans

1. Inleiding

Dit arrest van het Hof Arnhem-Leeuwarden is van belang, omdat met het arrest voor het eerst een bijzondere status wordt toegekend aan een smartphone. Volgens het gerechtshof brengt het analyseren van de gegevens op een smartphone een ernstige privacyschending met zich mee, omdat "*niet alleen toegang wordt verkregen tot verkeersgegevens, maar ook tot de inhoud van communicatie en privé-informatie van de gebruiker van de smartphone*". Daarmee zou de regeling tot inbeslagname van een voorwerp door een opsporingsambtenaar van art. 94 Sv niet voldoende kenbaar en voorzien zijn, aldus het hof.

Bijna een jaar eerder heeft het Hooggerechtshof van de Verenigde Staten in de lezenswaardige zaak *Riley/California* geoordeeld dat: *"Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life"*.[1] Om deze reden is volgens het Amerikaanse Hooggerechtshof een rechterlijk bevel vereist voor het kennisnemen van de gegevens op een smartphone. Overigens hoort bij een Amerikaanse 'warrant' niet alleen een machtiging van een rechter, maar moet ook nauwkeurig worden omgeschreven naar welke informatie wordt gezocht. Het is onduidelijk of het Gerechtshof Arnhem-Leeuwarden zich door deze uitspraak heeft laten inspireren, maar de *Riley*-zaak geeft goed aan hoe het vraagstuk over de wenselijkheid van een bijzondere bescherming van smartphones in meer landen speelt.

Het Gerechtshof Arnhem-Leeuwarden stelt terecht dat de inbeslagname van een smartphone en het uitlezen van gegevens op een smartphone een ernstige inbreuk maakt op art. 8 EVRM. Echter, de Nederlandse regeling voor inbeslagname en het analyseren van gegevens op een smartphone is mijns inziens niet zozeer in strijd met art. 8 EVRM wegens een gebrek aan kenbaarheid en voorzienbaarheid zoals het gerechtshof stelt. De Nederlandse regeling is in strijd met artikel 8 EVRM, omdat de huidige Nederlandse regeling geen voldoende waarborgen biedt, die wel worden vereist in recente jurisprudentie van het Europees Hof voor de Rechten van de Mens (hierna: EHRM). Het vonnis behandelt deze jurisprudentie met betrekking tot het analyseren van gegevens op geautomatiseerde werken van het EHRM helaas niet.

In deze noot wordt eerst kort de Nederlandse regeling voor inbeslagname van smartphones uiteengezet, waarna de meest relevante jurisprudentie van het EHRM wordt besproken. Daarnaast wordt een vergelijking gemaakt met het recente arrest van 11 februari 2015 van het Hof van Cassatie in België over de inbeslagname en het uitlezen van gegevens die staan opgeslagen op smartphones.

2. Wettelijk kader inbeslagname en onderzoek van opgeslagen gegevens

[1] U.S. Supreme Court 25 juni 2014, 573, p. 28 (*Riley/ California*). De uitspraak geeft ook interessante informatie over de opsporingspraktijk in de Verenigde Staten m.b.t. het in beslag nemen van gegevensdragers.

Naar huidig Nederlands recht bestaan er drie regelingen op basis waarvan een smartphone of andere 'gegevensdrager'[2] in beslag kan worden genomen. Binnen strafvordering worden gegevensdragers behandeld als elk ander voorwerp dat vatbaar is voor inbeslagneming en aan nader onderzoek kan worden onderworpen.[3]

Ten eerste kunnen smartphones die in het bezit zijn van een verdachte in beslag worden genomen in het kader van een opsporingsonderzoek bij verdenking van een strafbaar feit. Een opsporingsambtenaar is onder omstandigheden bevoegd tot inbeslagname.[4] Inbeslagname kan namelijk plaatsvinden op basis van de volgende vier gronden:

1. om de waarheid aan de dag te brengen;
2. om wederrechtelijk verkregen voordeel aan te tonen;
3. ter verbeurdverklaring; of
4. ter onttrekking aan het verkeer.[5]

Het berichtenverkeer op een smartphone kan bijvoorbeeld bewijs opleveren in een opsporingsonderzoek naar drugshandel en mag daarom in beslag worden genomen ten behoeve van de waarheidsvinding. De bevoegdheid tot inbeslagname impliceert dat de opgeslagen gegevens op andere gegevensdragers, zoals een smartphone, nader kunnen worden geanalyseerd.[6] In kinderpornozaken is het verder bijvoorbeeld mogelijk gegevensdragers in beslag te nemen op basis van verschillende gronden. De opgeslagen gegevens kunnen bijvoorbeeld worden geanalyseerd op kinderpornografische afbeeldingen ten behoeve van de waarheidsvinding. De daarop gevonden kinderporno kan vervolgens worden onttrokken aan het verkeer en de computerkast en andere onderdelen kunnen worden verbeurd verklaard.[7]

Ten tweede kunnen smartphones en andere gegevensdragers tijdens een doorzoeking van een plaats in beslag worden genomen.[8] Na inbeslagname kunnen de gegevens nader worden geanalyseerd. Afhankelijk van de locatie van het voorwerp gelden er meer of minder

---

[2] Het begrip 'gegevensdrager' wijkt af van het begrip 'geautomatiseerd werk' zoals gedefinieerd in art. 80sexies Sr. Een USB-stick kan bijvoorbeeld een gegevensdrager zijn, maar geen geautomatiseerd werk omdat het geen gegevens verwerkt en overdraagt. In het conceptwetsvoorstel Computercriminaliteit III wordt voorgesteld het begrip te wijzen, waarbij de cumulatieve vereisten van opslaan, overdragen en verwerken voor geautomatiseerde werken komt te vervallen. Een smartphone valt overigens nu ook al onder de definitie van een geautomatiseerd werk.

[3] Zie ook *Kamerstukken II* 1989/90, 21551, nr. 3, p. 12-13.

[4] Zie art. 56, 95, 96, 96a, 96b en 551 Sv. Zie art. 56, 96c, 97 en 100 Sv voor de voorwaarden van inbeslagname door de (hulp)officier van justitie.

[5] Zie art. 94. Zie ook de Aanwijzing inbeslagname, *Stcrt.* 2010, 19117.

[6] Zie F.P.E. Wiemans, 'Onderzoek van gegevens in geautomatiseerde werken', (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2004, p. 124. Zie ook het discussiedocument 'Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken (Boek 2)', versie 4 juli 2014), p. 37 met verwijzing naar HR 8 oktober 1985, ECLI:NL:HR:1985:AC0537. In het discussiedocument wordt opgemerkt dat op grond van art. 215la Sv gegevens waarover het verschoningsrecht zich uitstrekt moeten worden gescheiden (met verwijzing naar ECLI:NL:HR:2007:AZ3564 en ECLI:NL:HR:2013:CA0434).

[7] Zie ook punt 9, het 'Handvat afdoening gegevensdragers' van de Aanwijzing inbeslagname.

[8] Zie art. 96 Sv, art. 96b Sv, art. 96c Sv en art. 110 Sv.

waarborgen voor de doorzoeking. Bij een doorzoeking in een woning is een machtiging van een rechter-commissaris vereist.

Ten derde kunnen smartphones en andere geautomatiseerde werken tijdens een doorzoeking ter vastlegging van gegevens op een geautomatiseerd werk op een bepaalde plaats in beslag worden genomen en de opgeslagen gegevens op het voorwerp nader worden geanalyseerd.[9] De voorwaarden voor dit type doorzoeking zijn gekoppeld aan de reguliere regeling voor de doorzoeking.

In casu betreft deze zaak de eerste situatie waarbij een smartphone van de verdachte in beslag wordt genomen ten behoeve van de waarheidsvinding op grond van art. 94 Sv in het kader van een opsporingsonderzoek naar geweldpleging en mishandeling. De opsporingsambtenaar heeft na inbeslagname de gegevens op de smartphone onderzocht en daarbij een Whatsapp-gesprek uitgeprint. De inhoud van het Whatsapp-gesprek is aan het onderzoeksdossier toegevoegd. De verdediging stelt zich kort gezegd op het standpunt dat de inbeslagname van een smartphone en het analyseren van de gegevens op de smartphone door de opsporingsambtenaar onnodig en disproportioneel is geweest. Daarmee zou de handeling in strijd zijn met art. 8 EVRM.

Het Hof Arnhem-Leeuwarden accepteert het verweer in de zin dat de inbeslagname inderdaad in strijd wordt geacht met art. 8 EVRM. Door de ernstige privacyschending zou de huidige regeling van art. 94 Sv niet voldoende kenbaar en voorzienbaar voor de betrokkenen zijn. Aan het geconstateerde vormverzuim worden echter geen rechtsgevolgen toegekend, omdat de gegevens op de smartphone geen onderdeel van de bewijsconstructie van het gerechtshof vormt.

Het is de vraag of de wettelijke regeling voor de inbeslagname en het uitlezen van gegevens op een smartphone niet voldoende kenbaar en voorzienbaar is in Nederland. De Aanwijzing inbeslagneming legt namelijk de regeling voor inbeslagname van voorwerpen op grond van art. 94 Sv uitvoerig uit. Echter, gezien de ernstige inbreuk dat het analyseren van gegevens op inbeslaggenomen gegevensdragers met zich meebrengt kan – zoals de verdediging in casu ook stelt – de inbeslagname onder omstandigheden inderdaad disproportioneel en daarmee in strijd worden geacht in de zin van art. 8 EVRM. Bovendien wijst recente jurisprudentie van het EVRM ook op bepaalde vereiste waarborgen voor het onderzoeken van gegevens op geautomatiseerde werken. Daarbij is het de vraag is of het Nederlandse juridisch kader aan deze vereisten voldoet.

3. Artikel 8 EVRM en de bijzondere bescherming aan geautomatiseerde werken

In verschillende uitspraken wijst het EHRM erop dat het doorzoeken van een plaats en inbeslagname van computers een inbreuk maakt op het recht op privacy zoals bedoeld wordt

[9] Zie art. 125i Sv jo. art. 96b Sv, art. 125i Sv jo. art. 96c Sv en art. 125i Sv jo. art. 110 Sv of art. 97 Sv. Zie ook *Kamerstukken II* 2003/04, 29441, nr. 3, p. 11.

in art. 8 EVRM. In het bijzonder wordt daarbij een inbreuk gemaakt op het recht op vertrouwelijke correspondentie en het recht op privéleven binnen de woning als onderdeel van het recht op privacy zoals is omschreven in art. 8 lid 1 EVRM.[10] Eerder hebben auteurs zoals Groothuis en De Jong al opgemerkt dat het analyseren van gegevens op computers een ernstige inbreuk op art. 8 EVRM met zich meebrengt.[11]

In de meest recente uitspraak *Prezhdarovi/Bulgarije*[12] merkt het EHRM expliciet op dat het nationale recht van verdragstaten voldoende waarborgen moet bevatten tegen de willekeurige inmenging met art. 8 EVRM door nationale overheden.[13] Meer specifiek bestaan deze vereiste waarborgen uit:

1. een (bij voorkeur voorafgaande) autorisatie van een onderzoeksrechter;[14]
2. een beperking van de reikwijdte van de zoeking in de computer.[15]

Met betrekking tot de beperking van het onderzoek aan de opgeslagen persoonsgegevens van de inbeslaggenomen computers neemt het EHRM uitdrukkelijk in aanmerking dat:

"the court that approved the measure did not consider the scope of the operation and did not make a distinction between information which had been necessary for the investigation and information which had not been relevant."[16]

De zaak *Prezhdarovi/Bulgarije* heeft betrekking op de situatie van een doorzoeking van een plaats, waarbij de gegevens op computers na inbeslagname worden geanalyseerd. De verdachte heeft ook uitdrukkelijk beklag ingesteld tegen de inbeslagname. In casu betreft het echter de inbeslagname van een smartphone, waarna de gegevens op een smartphone worden geanalyseerd. Mijns inziens is de privacyinbreuk op art. 8 EVRM echter hetzelfde, omdat de privacyinbreuk betrekking heeft op de analyse van de gegevens op een inbeslaggenomen smartphone. De vereiste waarborgen van een machtiging van een onderzoeksrechter en beperking van de reikwijdte van de zoeking op het geautomatiseerde werk zouden daarom ook voor de zoeking op een smartphone na inbeslagname moeten gelden. Door het stellen van deze vereisten voor het juridische kader voor het doorzoeken van gegevens op geautomatiseerde werken kent het EHRM een bijzondere bescherming toe aan computers.

---

[10] Zie EHRM 27 september 2005, nr. 50882/99, § 71 (*Petri Sallinen e.a./ Finland*), EHRM 7 oktober 2007, nr. 74336/01, § 42-46 (*Wieser en Bicos Beteiligungen GmbH/ Oostenrijk*) en EHRM 14 maart 2013, nr. 24117/08, § 105 (*Bernh Larsen Holding AS e.a./Noorwegen*) en EHRM 30 september 2014, nr. 8429/05, § 41 (*Prezhdarovi/Bulgarije*).

[11] Zie M.M. Groothuis & T. de Jong, 'Is een nieuw grondrecht op integriteit en vertrouwelijkheid van ICT-systemen wenselijk?', *P&I* 2010, nr. 6, p. 280.

[12] EHRM 30 september 2014, nr. 8429/05 (*Prezhdarovi/Bulgarije*).

[13] EHRM 30 september 2014, nr. 8429/05, § 44 (*Prezhdarovi/Bulgarije*).

[14] EHRM 30 september 2014, nr. 8429/05, § 45-46 (*Prezhdarovi/Bulgarije*).

[15] EHRM 30 september 2014, nr. 8429/05, § 49 (*Prezhdarovi/Bulgarije*). Zie ook § 50: *"The Court finds that the lack of clear rules regarding the scope of the judicial review in such a situation, combined with the lack of any meaningful review of the lawfulness of and the justification for the measure, rendered the post factum judicial review ineffective for the purposes of the protection of the applicants' rights as guaranteed by Article 8 of the Convention."*

[16] EHRM 30 september 2014, nr. 8429/05, § 49 (*Prezhdarovi/Bulgarije*).

Met betrekking tot de Nederlandse regeling voor inbeslagname van gegevensdragers en het uitlezen van opgeslagen gegevens op de gegevensdragers zou deze uitspraak mijns inziens tot gevolg moeten hebben dat voortaan: (1) een machtiging van een rechter-commissaris is vereist voor de inbeslagname van computers (geautomatiseerde werken); en (2) de reikwijdte van het onderzoek van de opgeslagen gegevens op computers uitdrukkelijk wordt beperkt door een proportionaliteitstoets. Op welke manier deze regeling moet worden aangepast behoeft nader onderzoek. Daarbij moet ook aandacht worden besteed aan praktische en technische uitvoerbaarheid. Gedacht kan worden aan het creëren van een aparte regeling voor de inbeslagname en het onderzoek op gegevensdragers in het Wetboek van Strafvordering of in een Algemene Maatregel van Bestuur.

4. Vergelijking met situatie België

België heeft recentelijk een geheel andere benadering gekozen. Op 11 februari 2015 heeft het Hof van Cassatie zich namelijk uitgesproken over de procedurele voorwaarden voor het uitlezen van 'informaticasystemen', waar ook smartphones onder vallen. Dit arrest is tevens opgenomen in dit nummer van *Computerrecht*.[17]

Het Hof van Cassatie stelt dat het kennisnemen van gegevens op een informaticasysteem in het verlengde ligt van de beslagbevoegdheid. Daarmee zouden geen bijkomende voorwaarden zoals een gerechtelijk bevel zijn vereist. Vanwallaghem wijst op het feit dat in België (en overigens ook in Nederland) opgeslagen gegevens op in beslag genomen computers al jaren kunnen worden uitgelezen zonder tussenkomst van een onderzoeksrechter.[18] Privacygevoelige informatie is ook te vinden in een papieren agenda of een portefeuille, waarvoor nooit bijzondere waarborgen voor zijn vereist. Een verschil in rechtsbescherming zou daarom volgens de auteur niet gewenst zijn.

Conings stelt in haar noot in twijfel dat de bevoegdheid tot het doorzoeken van gegevens op een informaticasysteem kan worden afgeleid uit de beslagbevoegdheid.[19] De belangrijkste reden daarvoor is dat het uitlezen van gegevens op informaticasystemen een ernstige inbreuk op het recht op privacy maakt, hetgeen niet vergelijkbaar is met de inbeslagname van andere voorwerpen. Met verwijzing naar de jurisprudentie van het EHRM met betrekking tot het analyseren van gegevens op computers stelt Conings mijns inziens terecht dat de benadering van het Hof van Cassatie moeilijk verdedigbaar is in het licht van art. 8 EVRM.[20]

Het Belgische arrest is tegengesteld aan het arrest van het Hof Arnhem-Leeuwarden in de zin dat het Nederlandse gerechtshof wel een bijzondere status toekent aan smartphones. Echter,

---

[17] De uitspraak is eerder kort behandeld door Charlotte Conings in de rubriek Strafrecht & ICT in *Computerrecht* 2015/112.
[18] Zie P. Vanwallaghem, 'Onderzoeksrechter moet niet tussenkomen voor uitlezen gsm', *Juristenkrant* 2015, afl. 307, p. 2.
[19] C. Conings, 'Het uitlezen van een gsm of ander privaat IT-systeem: This is not America' (noot onder Cass. 11 februari 2015), *RW* 2015, n.t.v.).
[20] Zie uitgebreid: C. Conings, 'Het uitlezen van een gsm of ander privaat IT-systeem: This is not America' (noot onder Cass. 11 februari 2015), *RW* 2015, n.t.v.).

ook de Nederlandse rechter gaat niet zover dat bijvoorbeeld een machtiging van een rechter-commissaris verplicht wordt gesteld voor het analyseren van gegevens op een in beslag genomen smartphone. Deze eis lijkt, zoals in onderdeel 3 uiteen is gezet, echter wel kunnen worden afgeleid uit jurisprudentie van het EHRM.

5. Slotoverweging

Het arrest van het Hof Arnhem-Leeuwarden geeft voor het eerst een bijzondere status aan smartphones binnen het Nederlandse strafrecht. Deze aparte status voor smartphones is mijns inziens terecht gezien de ernstige privacy-inbreuk die plaatsvindt, indien smartphones in beslag worden genomen en de opgeslagen gegevens vervolgens worden uitgelezen. Bovendien wijst recente jurisprudentie van het EHRM op specifieke waarborgen voor de nationale wetgeving van verdragsstaten dat het analyseren van gegevens op geautomatiseerde werken mogelijk maakt.

In het kader van het project 'Modernisering strafvordering' wordt in het discussiedocument omtrent de Nederlandse regeling voor inbeslagname en doorzoeking door de auteurs van het Ministerie van Veiligheid en Justitie erkend dat het doorzoeken van gegevens op computers een ernstige inbreuk maakt op het recht op privacy.[21] In het discussiedocument wordt voorgesteld een aparte afdeling in het Wetboek van Strafvordering te maken voor 'onderzoek van gegevensdragers en in geautomatiseerde werken', hetgeen zowel de situatie van een doorzoeking als inbeslagname zou omvatten. Daarbij wordt overwogen dat een bevel van de officier van justitie altijd op zijn plaats is en voor de kennisname van gegevens met inhoud van communicatie ook een machtiging van een rechter-commissaris vereist zou moeten zijn.[22]

De bovenstaande korte analyse van de jurisprudentie van het EHRM laat echter zien dat de machtiging van de rechter-commissaris wellicht in alle gevallen bij het analyseren van gegevens op geautomatiseerde werken na inbeslagname op zijn plaats is. Het verdient aldus aanbeveling om in de voorgestelde nieuwe regeling voor onderzoek van gegevens op gegevensdragers en geautomatiseerde werken de vereiste waarborgen die zijn geformuleerd in jurisprudentie van het EHRM mee te nemen.

[21] Zie het discussiedocument van 4 juli 2014, 'Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken', p. 37.
[22] Zie het discussiedocument van 4 juli 2014, 'Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken', p. 51-53.