J.J. Oerlemans & B. Schermer[1]

Strafrechtelijke aspecten van implantaten in het lichaam

Computerrecht 2022/4

Dit artikel gaat over de strafrechtelijke aspecten van implantaten en geïntegreerde apparaten in het lichaam, zoals bionische ledematen en mens-machine interfaces. Enerzijds wordt nagegaan hoe het strafrecht kan reageren op strafrechtelijke gedragingen gericht op deze apparaten en anderzijds wordt verkend welke grenzen het strafrecht kan stellen aan opsporingshandelingen met betrekking tot implantaten en in het lichaam geïntegreerde apparaten.

1. Inleiding

Mensen gebruiken al duizenden jaren technologie om lichamelijke ongemakken of beperkingen het hoofd te bieden. Denk bijvoorbeeld aan de leesbril of de wandelstok. Naarmate de technologie zich verder ontwikkelde, werd het mogelijk om meer geavanceerde (medische) hulpmiddelen duurzaam met ons lichaam te verbinden en zelfs te implanteren. Bekende voorbeelden van medische implantaten zijn gehoorimplantaten, pacemakers en hersenstimulatoren. Hoewel het nog wat verder in de tijd ligt, gaan onderzoekers ervan uit dat het ook mogelijk wordt om computers aan te sturen met behulp van ons brein. Het zou dan bijvoorbeeld mogelijk zijn prothesen te bedienen met een computer in het brein of met onze gedachten zoekslagen te maken op internet ('cyber thinking'). In 2021 maakte het bedrijf *Neuralink* van tech-icoon Elon Musk een technologische sprong door een chimpansee met behulp van een brein-machine interface het computerspel *Pong* te laten spelen met zijn gedachten.[2]

Met deze ontwikkelingen komen we steeds dichter bij het punt dat implantaten en prothesen niet meer alleen gericht zijn op het herstellen van beperkingen, maar ook gericht kunnen worden op het uitbreiden of verbeteren van de mogelijkheden van ons lichaam en onze geest. Zoals de Commissie-Koops in 2018 signaleerde openen deze technologieën "*de weg voor menselijke 'augmentatie': het vrijwillig vervangen van bijvoorbeeld ledematen door sterkere kunstmatige varianten, of zintuigen als zicht, gehoor, geur en smaak door kunstmatige zintuigen*".[3] Net als al veel eerder in het *science fiction*-genre is gesignaleerd verwachten wij dat het een kwestie van tijd is tot deze technologieën – met alle gevolgen van dien – werkelijkheid worden.[4]

In paragraaf 2 verkennen wij of het materieel strafrecht in Nederland voldoende is uitgerust om mensen bescherming te bieden tegen cyberdreigingen met betrekking tot implantaten en andere geïntegreerde apparaten in het lichaam. Daarnaast onderzoeken wij in paragraaf 3 of aanpassingen in het formele strafrecht ('strafvordering') noodzakelijk zijn. Overheidsinstanties kunnen namelijk ook gebruikmaken van implantaten en andere geïntegreerde apparaten in het lichaam ten behoeve van de opsporing. Dat maakt een grote inbreuk op de fundamentele rechten van de betrokkene, waardoor het noodzakelijk is duidelijke grenzen te trekken bij dergelijke overheidsinmengingen om misbruik van bevoegdheden tegen te gaan en fundamentele rechten van de betrokkenen te beschermen. Het artikel sluit af met enkele aanbevelingen voor de wetgever.

2. Materieel strafrecht

Digitale technologieën integreren steeds verder in en met het menselijk lichaam. Dit biedt nieuwe kansen voor cybercriminelen en andere kwaadwillenden. Hieronder bespreken wij enkele delicten die in de toekomst te verwachten zijn en verkennen wij hun strafbaarstelling.

2.1 *Hacking*

Gasson & Koops (2013) stellen dat het aanvallen van genetwerkte technologie in het menselijk lichaam 'de volgende stap in de evolutie van cybercriminaliteit' is.[5] Het meest ernstige en spectaculaire scenario, onder andere gedramatiseerd in de populaire tv-serie *Homeland*, is dat een pacemaker van buitenaf wordt gehackt om een dodelijke hartaanval te veroorzaken.[6] Het is namelijk bekend dat sommige pacemakers kwetsbaar zijn voor hackaanval-

1 Prof. mr. dr. J.J. Oerlemans is bijzonder hoogleraar inlichtingen en recht bij het Willem Pompe Instituut voor Strafrechtwetenschappen en het Montaigne Centrum voor Rechtsstaat en Rechtspleging van de Universiteit Utrecht. Prof. mr. dr. B.W. Schermer is hoogleraar privacy en cybercrime bij het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden (eLaw@Leiden) en partner bij juridisch adviesbureau Considerati. Dit artikel bouwt voort op onze bijdrage 'Cyberpunk' is now: de strafrechtelijke aspecten van menselijke augmentatie' in het liber amicorum Meesterlijk voor Jaap van Herik (red. B.H.M. Custers, F. Dechesne & S. van der Hof, Leiden, 2021, p. 151-160).

2 Nu.nl, 'Aap leert spelletje Pong spelen met alleen zijn gedachten', 9 april 2021.

3 Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018 (hierna: Commissie-Koops 2018), p. 18. Bart Schermer is lid geweest van de Commissie-Koops.

4 Zie bijvoorbeeld William Gibson, *Neuromancer*, Ace, 1984 en het verhaal 'We Can Remember It For You Wholesale' door Philip K. Dick (eerst verschenen in 1966) en o.a. gepubliceerd in *Selected Stories of Philip K. Dick*, Random House 2002.

5 M.N. Gasson & B.J. Koops, 'Attacking human implants: a new generation of cybercrime', *Law, Innovation and Technology* 2013, *5*(2), p. 248-277.

6 Dat lijkt overigens nog eenvoudiger met een Implanteerbare Cardioverter Defibrillator (ICD) die ook wel wordt ingezet als mensen eerder door een hartstilstand zijn getroffen.

len.[7] Met deze kennis in het achterhoofd was het zo gek nog niet dat vicepresident Dick Cheney in 2007 al zijn pacemaker aanpaste om aanvallen van buitenaf te weren.[8]

Pacemakers vallen, net als alle andere apparaten die met netwerken kunnen worden verbonden, onder het begrip 'geautomatiseerd werk' zoals beschreven in artikel 80sexies van het Wetboek van Strafrecht (Sr).[9] Het opzettelijk en wederrechtelijk binnendringen daarvan is strafbaar als computervredebreuk op grond van artikel 138ab Sr. Als daadwerkelijk een persoon opzettelijk van het leven wordt beroofd, kan er sprake zijn van doodslag (artikel 287 Sr), of moord als dat met voorbedachten rade plaatsvindt (artikel 289 Sr). Als de computervredebreuk of beschadiging van het medisch implantaat de dood tot gevolg heeft, kan ook onderdeel 3 van artikel 161sexies Sr ten laste worden gelegd (het verstoren van de werking van een geautomatiseerd werk de dood ten gevolge hebbend). Op dit laatste delict staat een maximale gevangenisstraf van 15 jaar.

2.2 *Manipuleren van gegevens in het implantaat*

Het opzettelijk en wederrechtelijk wijzigen van de functionaliteiten van medische implantaten, zoals het harder of zachter zetten van een gehoorapparaat, is eveneens strafbaar (artikel 138ab Sr). Net als het zonder toestemming aftappen of overnemen van het signaal (artikel 138ab lid 2 Sr en artikel 139c Sr).[10] Het is ook denkbaar dat een medisch implantaat onbruikbaar wordt gemaakt door het te overladen met gegevens (ook wel een *denial-of-service* aanval genoemd), hetgeen strafbaar is gesteld in artikel 138b Sr.

Denkbaar is ook dat medische implantaten gegijzeld worden voor losgeld. Net zoals laptops en servers gehackt en gegijzeld kunnen worden door kwaadaardige software (ransomware), is dat ook mogelijk bij medische implantaten. De bedreiging het apparaat uit te schakelen kan daarbij als extra stimulans werken om het losgeld te betalen. Het installeren van kwaadaardige software (malware) is specifiek strafbaar gesteld in artikel 350a lid 1 en artikel 350c Sr, maar uiteraard kan ook aan een regulier delict als afpersing (artikel 317 Sr) worden gedacht. Wanneer de werking van het medische implantaat wordt gehinderd door de ransomware, komen ook delicten als zware mishandeling (artikel 302 Sr) in beeld.

Voor prothesen en implantaten die via het zenuwsysteem verbonden zijn, zijn er aanvullende dreigingen. Zo kunnen bionische ledematen mogelijk op afstand worden bestuurd. Allereest kan de 'drager' hierdoor pijn ervaren en letsels oplopen. Het delict mishandeling is daarbij mogelijk van toepassing (artikel 300-303 Sr). Afhankelijk van de gevolgen staat daarop een maximale gevangenisstraf van 3 tot 15 jaar. Maar het overnemen van prothesen en implantaten kan ook gevaar opleveren voor derden.[11] Denk bijvoorbeeld aan het overnemen van iemands bionische arm tijdens het autorijden of het slaan van personen met een op afstand bestuurbare bionische arm.

De gevolgen van computervredebreuk en sabotage kunnen groter zijn als het om apparaten gaat die verbonden zijn met het brein. Echter, voor de strafbaarstellingen wijzigt er niet veel ten opzichte van het voorgaande. Wel wordt het wellicht mogelijk om valse herinneringen in iemands brein te plaatsen, of bestaande herinneringen te verwijderen of wijzigen. Hiermee kan ook het gedrag van een persoon worden beïnvloed.[12] In science fiction-literatuur en -films, zoals *Bladerunner* (1982), zijn dit soort mogelijkheden al veel eerder overwogen. Voor dergelijke vergrijpen zijn zeer waarschijnlijk (nieuwe) delictsomschrijvingen nodig met serieuze strafbedreigingen, omdat hier de kern van de persoonlijke integriteit en de menselijke waardigheid wordt aangetast.

2.3 *Diefstal en vernieling*

Het is niet ondenkbaar dat er in de toekomst een lucratieve markt ontstaat voor gestolen implantaten en prothesen. Naar verwachting zullen implantaten en prothesen die onze bestaande lichaamsfuncties verbeteren zeer kostbaar zijn en daarmee interessant voor criminelen. Ook is het mogelijk om prothesen en implantaten (opzettelijk) te beschadigen.

Diefstal van bionische ledematen en implantaten kwalificeert uiteraard als diefstal (artikel 310 Sr), omdat daarbij opzettelijk en wederrechtelijk voorwerpen worden weggenomen. Wanneer geweld wordt gebruikt om een prothese te stelen, denk bijvoorbeeld aan een bionische arm die in een beroving van het lichaam wordt getrokken, kan ook het delict 'diefstal met geweld' ten laste worden gelegd (artikel 312 Sr). Degene die een gestolen prothese of implantaat koopt kan het delict (opzet)heling (artikel 416 Sr) ten laste worden gelegd. Voor het opzettelijk beschadi-

7 Zie bijvoorbeeld D. Halperin et al., 'Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses', *Security and Privacy* 2008, p. 129-142.

8 Zie D. Goodin, 'Dick Cheney altered implanted heart device to prevent terrorist hack attacks', *Ars Technica*, 19 oktober 2013.

9 Artikel 80sexies Sr: Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken. In de Wet computercriminaliteit III (*Stb.* 2018, 322) is het artikel aangepast. In de toelichting wordt duidelijk gemaakt dat apparaten als onderdeel van het 'Internet of Things' en pacemakers onder het begrip vallen (*Kamerstukken II* 2015/16, 34372, nr. 3, p. 85-86). Zie ook Commissie-Koops 2018, p. 79. Ook een chip in een implantaat kan als geautomatiseerd werk worden gezien. Zie in dat kader Rb. Midden-Nederland 17 juni 2020, ECLI:NL:RBMNE:2020:2277, *Computerrecht* 2020/185, m.nt. J.J. Oerlemans.

10 Zie ook B.W. Schermer, 'High tech crime en ambient intelligence', *Computerrecht* 2010/173.

11 Zie ook M.N. Gasson & B.J. Koops, 'Attacking human implants: a new generation of cybercrime', *Law, Innovation and Technology* 2013, *5*(2), p. 263.

12 M.N. Gasson & B.J. Koops, 'Attacking human implants: a new generation of cybercrime', *Law, Innovation and Technology* 2013, *5*(2), p. 266.

gen van een prothese of implantaat is artikel 350 Sr relevant.

Een interessante vraag is of het stelen of beschadigen van een prothese ook kan kwalificeren als mishandeling (artikel 300 Sr) of zware mishandeling (artikel 302 Sr). Wil er sprake zijn van een mishandeling dan moet er ten minste sprake zijn van een 'min of meer hevige onlust veroorzakende gewaarwording in of aan het lichaam'.[13] De vraag is daarbij hoe wij de zinsnede 'in of aan het lichaam' moeten interpreteren. Vormt een prothese een onderdeel van ons lichaam en strekt de lichamelijke integriteit zich daarmee ook uit tot deze prothesen? Naar ons oordeel zal de diefstal of beschadiging van een bionische ledemaat in veel gevallen tot een 'hevige onlust veroorzakende gewaarwording' leiden aan het daadwerkelijke lichaam (de bionische arm die met geweld van het lichaam wordt getrokken in een beroving). In dat geval kan er sprake zijn van mishandeling. Naar verwachting zal er in een dergelijk scenario wel sprake zijn van eendaadse samenloop, waardoor in de praktijk waarschijnlijk diefstal met geweld de meest voor de hand liggende keuze lijkt in een tenlastelegging.

Het is echter twijfelachtig dat ook sprake is van zware mishandeling door de diefstal of beschadiging van een prothese. Waarschijnlijk wordt geen blijvend zwaar letsel toegebracht aan het slachtoffer wanneer bijvoorbeeld een bionische arm wordt gestolen of beschadigd. Hoewel de gebruiker op dat moment ontegenzeggelijk minder fysieke mogelijkheden heeft, kan deze situatie met een nieuwe bionische arm mogelijk worden hersteld. De dader heeft het lichaam als het ware teruggebracht in haar originele fysieke positie (die van voor de augmentatie). Hierdoor kan het bestanddeel 'zwaar lichamelijk letsel' waarschijnlijk niet bewezen worden.

Bij het stelen van implantaten zal er nagenoeg altijd sprake zijn van het toebrengen van (zwaar) lichamelijk letsel, omdat het implantaat uit het lichaam moet worden gehaald. In dit geval is er dus nagenoeg altijd sprake van (zware) mishandeling, los van het feit dat om een implantaat tegen iemands wil te verwijderen waarschijnlijk ook delicten als wederrechtelijke vrijheidsberoving (artikel 282 Sr) gepleegd moeten worden.

2.4 *Beschouwing materieelrechtelijke bepalingen*

Het bovenstaande overzicht aan bedreigingen en strafbaarstellingen laat zien dat er voor een deel sprake is van 'old crimes with new tools', oftewel bestaande delicten worden gepleegd met behulp van nieuwe technologische middelen.[14] Aan de genoemde strafbaarstellingen voor hacking van implantaten, bionische ledematen en mens-machine interfaces valt op dat hoge gevangenisstraffen slechts van toepassing zijn als het fysieke beschadiging of zelfs de dood tot gevolg heeft. Voor de reguliere computerdelicten is vaak maximaal vier jaar gevangenisstraf van toepassing en zijn slechts strafverzwaringen van toepassing als grote hoeveelheden apparaten worden aangetast, de apparaten onderdeel van een vitale infrastructuur zijn, of als de aanval kwalificeert als terroristisch misdrijf.[15]

Het belangrijke verschil bij het type delicten dat wij hier bespreken is dat de meeste van deze delicten gericht zijn tegen apparaten *in* het menselijk lichaam in plaats van apparaten *buiten* het menselijk lichaam. Het verschil zit met name in de aantasting van de lichamelijke integriteit als wordt binnengedrongen in apparaten in het menselijk lichaam. In navolging van Gasson & Koops (2013, p. 274) pleiten wij daarom voor de invoering van een hogere maximale gevangenisstraf als in apparaten *in* het menselijk lichaam wordt binnengedrongen. Dit doet recht aan de aantasting van de lichamelijke integriteit van het slachtoffer en de ernstige schade die daarmee gepaard kan gaan. Meer concreet verdient het de overweging het plegen van computerdelicten gericht op 'in of met het lichaam verbonden geautomatiseerde werken' als strafverzwarende omstandigheid aan artikel 138b Sr toe te voegen.

Tegelijkertijd tekenen we daarbij aan dat het strafrecht een ultimum remedium is en een strafverzwaring slechts beperkt een bijdrage levert aan de bestrijding van deze vorm van misdaad. Juist ook het stellen van kwaliteits- en beveiligingseisen voor implantaten, bionische ledematen en mens-machine interfaces (*security-by-design*), zullen de mogelijkheden van misbruik door derden beperken.[16]

3. Formeel strafrecht

Implantaten, genetwerkte prothesen en mens-machine interfaces kunnen waardevolle informatie voor de opsporing bevatten. De Commissie-Koops, die onderzoek heeft gedaan naar 'strafvordering in het digitale tijdperk', wijst bijvoorbeeld op de grote waarde van audiogegevens die worden opgeslagen in een cochleair implantaat (eenvoudig gezegd een geavanceerd gehoorapparaat).[17]

In deze paragraaf behandelen wij de normering van opsporingsmethoden met betrekking tot implantaten en andere geïntegreerde apparaten in het lichaam. Het gaat om: (1) de inbeslagname van apparaten in en aan het menselijk lichaam, (2) het uitlezen van hersensignalen, (3) het hacken van apparaten in het menselijk lichaam, en (4)

13 HR 9 september 2014, ECLI:NL:HR:2014:2677, *NJ* 2014/402, m.nt. red. en *NBSTRAF* 2014/241, m.nt. van J.S. Nan.

14 Zie ook B.W. Schermer, 'High tech crime en ambient intelligence', *Computerrecht* 2010/173.

15 Zie artikel 138b Sr en artikel 350c Sr.

16 Deze vereisten vloeien ook voort uit bestaande wetgeving zoals de Algemene Verordening Gegevensbescherming (meer specifiek artikel 25 en 32 AVG) en de Verordening medische hulpmiddelen (meer specifiek artikel 17 MDR).

17 Commissie-Koops 2018, p. 18.

de mogelijkheid tot het traceren van apparaten in het menselijk lichaam.

3.1 *De inbeslagname van apparaten in en aan het menselijk lichaam*

Computers worden binnen de strafvordering in principe net als elk ander voorwerp beschouwd. Voorwerpen kunnen tijdens een doorzoeking in beslag worden genomen ten behoeve van de waarheidsvinding en kunnen daarmee als bewijs dienen. Voor een doorzoeking in een woning en de inbeslagname van computers is een bevel van een officier van justitie en een machtiging van een rechter-commissaris noodzakelijk,[18] terwijl voor een doorzoeking van een kantoor en de inbeslagname van een computer slechts een bevel van de officier noodzakelijk is (zie artikel 96c Wetboek van Strafvordering (Sv)).

Toch kan bij de inbeslagname van computers en met name bij het uitlezen van de gegevens op computers er een ernstige privacy-inbreuk plaatsvinden, waardoor meer waarborgen op zijn plaats zijn. De Hoge Raad heeft in het bekende 'smartphone-arrest' uit 2017 duidelijk gemaakt dat bij de inbeslagname van computers minstens een bevel van een officier van justitie of machtiging van een rechter-commissaris is vereist, voor zover daarbij een "min of meer volledig beeld van bepaalde aspecten uit het persoonlijk leven van de verdachte" wordt verkregen.[19] Als bijvoorbeeld een smartwatch in beslag wordt genomen en daar onderzoek aan wordt gedaan, dan is er sneller sprake van stelselmatigheid gezien alle gezondheidsgegevens (bloeddruk, hartslag of suikerspiegel) die op het apparaat te vinden zijn.[20] Deze gegevens geven namelijk een min of meer compleet beeld van een bepaald aspect van iemands persoonlijke leven (in casu de gezondheid). Daarnaast zijn gezondheidsgegevens sowieso gevoeliger dan 'gewone' persoonsgegevens.

Inbeslagname van een implantaat of een apparaat dat geïntegreerd is in het menselijk lichaam is een serieuze inbreuk op de lichamelijke integriteit van de betrokkene. De Commissie-Koops (2018, p. 99) wijst ook nadrukkelijk op dit spanningsveld met de lichamelijke integriteit, waardoor speciale waarborgen in het Wetboek van Strafvordering overwogen moeten worden. Met een schakelbepaling bij een bepaling over 'onderzoek in of aan onlosmakelijk met het lichaam geautomatiseerde werken' naar de regeling voor 'onderzoek aan of in het lichaam', kan de regeling over onderzoek aan of in het lichaam van toepassing worden verklaard.[21] Een dergelijke schakelbepaling is nodig, omdat het onderzoek 'aan of in de chip' of 'met het lichaam geïntegreerde digitale gegevensdragers of geautomatiseerde werken' niet vanzelf onder onderzoek aan of in het lichaam valt. Ook al hoeft voor het uitlezen van dergelijke gegevensdragers niet per se in het lichaam te worden binnengedrongen, de inbreuk op de lichamelijke integriteit is volgens de Commissie-Koops wel vergelijkbaar met de inbreuk van onderzoek in het lichaam, zoals het inwendig schouwen of het verrichten van niet-invasief beeldvormend onderzoek.[22]

De Commissie-Koops suggereerde dat dit alleen zou mogen bij verdachten in opsporingsonderzoeken naar ernstige misdrijven met een gevangenisstraf van vier jaar of meer, met minstens een bevel van een officier van justitie. Als er een geen arts nodig is (omdat het onderzoek buiten het lichaam kan plaatsvinden) en geen gezondheidsrisico oplevert, zoals het van buitenaf uitlezen van onderhuids geïmplementeerde chips, zou het eventueel ook in opsporingsonderzoek naar andere misdrijven en bij derden mogelijk kunnen zijn. Wij sluiten ons erbij aan dat het een dergelijke regeling noodzakelijk is. De wetgever moet dan bepalen of een bevel van een officier van justitie of een machtiging van een rechter-commissaris daarbij noodzakelijk is.

In de meeste gevallen zal het voor de politie gelukkig ook praktischer zijn om het implantaat op enige afstand uit te lezen. Maar zelfs als een implantaat op afstand wordt uitgelezen, is er volgens ons nagenoeg altijd sprake van een aantasting van de lichamelijke integriteit en een ernstige inbreuk op het recht op privacy. Naast de gevoelige gegevens die het implantaat doorgaans bevat, is het uitlezen op zichzelf al een inbreuk op de lichamelijke integriteit van de betrokkene, omdat het apparaat als het ware onderdeel uitmaakt van het menselijk lichaam en tegen de wens van de verdachte wordt benaderd. Ditzelfde geldt naar ons oordeel voor het uitlezen en in beslag nemen van apparaten die duurzaam aan het menselijk lichaam zijn verbonden zoals bionische armen of kunstogen. In 2005 wezen Koops en Prinsen in het Nederlands Juristenblad (NJB) al op dit fundamentele verschil met de reguliere inbeslagname van voorwerpen en het uitlezen van computers.[23]

3.2 *Uitlezen van hersensignalen*

De Commissie-Koops signaleert dat het in de toekomst mogelijk wordt om – tot op zekere hoogte – hersensignalen van buitenaf uit te lezen.[24] Het is duidelijk dat met her-

18 Zie o.a. artikel 97 Sv.
19 HR 4 april 2017, ECLI:NL:HR:2017:584. Zie voor kritiek hierop, o.a., S. Royer & J.J. Oerlemans, 'Naar een nieuwe regeling voor beslag op gegevensdragers', *Computerrecht* 2017/200, p. 277-284. Zij stellen dat bij de inbeslagname en het uitlezen van gegevensdragers altijd een ernstige inbreuk in het recht op privacy van de betrokkene plaatsvindt.
20 Zie ook Commissie-Koops 2018, p. 100.
21 Commissie-Koops 2018, p. 100. De regeling over 'onderzoek aan of in het lichaam' staat in artikel 2.6.4.1 in het beoogde nieuwe Wetboek van Strafvordering.
22 Commissie-Koops, p. 99-100.
23 B.J. Koops & M.M. Prinsen, 'Glazen woning, transparant lichaam. Een toekomstblik op huisrecht en lichamelijke integriteit', *NJB* 2005, p. 624-630.
24 Commissie-Koops 2018, p. 101.

senlezen informatie wordt verkregen over het brein van de betrokken persoon. Deze informatie kan iets zeggen over iemands neurale gezondheid, emoties, of mentale toestand. Het zal niet verrassend zijn dat het verwerken van deze persoonsgegevens in de context van het strafrecht een inbreuk maakt op het recht op privacy uit artikel 8 EVRM.[25]

Verschillende auteurs, zoals Van Toor en Ligthart, wijzen in publicaties over 'neurorechten en strafrecht' ook op spanning met andere fundamentele rechten bij het uitlezen van hersensignalen. Het gaat dan met name om het recht op de vrijheid van gedachten en overtuigingen, het zwijgrecht en het nemo tenetur-beginsel (het recht van een verdachte niet mee te werken aan zijn eigen veroordeling).[26] Hoewel het nemo tenetur-beginsel niet expliciet is verankerd in ons nationale strafprocesrecht, is het wel af te leiden uit artikel 6 EVRM.[27] Bij het uitlezen van hersensignalen wordt de autonomie van de verdachte aangetast. Ligthart en Van Toor wijzen ook op het belang van de 'mentale privacy', in de zin dat elk individu zelf moet kunnen bepalen wie hij toelaat tot de intieme sfeer van zijn mentale leven – hoe triviaal een herinnering of opvatting ook is.[28]

Kort gezegd vormt onderzoek van hersensignalen een potentieel dermate ingrijpende inbreuk op de fundamentele rechten van de betrokkene, dat dit onder de huidige en voorgestelde regeling uitgesloten is voor opsporingsdoeleinden.[29] Wij zijn van mening dat in de toekomst overwogen moet worden of dergelijke methoden van waarheidsvinding überhaupt wenselijk zijn en zo ja, onder welke omstandigheden.[30] In deze afweging moeten ook andere fundamentele rechten dan het recht op privacy worden betrokken, zoals door onder andere Van Toor en Ligthart overtuigend uiteen is gezet.

Uiteindelijk is het aan de wetgever om via ons democratisch proces de grenzen aan te geven, als de onderzoekmethode in het kader van opsporingsonderzoeken toch wordt overwogen. Gegeven de gevoeligheid zou het parlement zich tot die tijd ook via een motie kunnen uitspreken voor een voorlopig expliciet verbod op het uitlezen van hersensignalen. Na verder onderzoek zal nader moeten worden bepaald waar de grenzen moeten liggen en welke regeling wij daarvoor moeten opnemen in ons Wetboek van Strafvordering.

3.3 *Hacken van apparaten in het menselijk lichaam*

Per 1 maart 2019 is het in Nederland mogelijk om in het kader van een opsporingsonderzoek naar ernstige misdrijven[31] die een ernstige inbreuk op de rechtsorde opleveren en wanneer het onderzoek dat dringend vordert, een geautomatiseerd werk te hacken.[32] De hackbevoegdheid kan in theorie dus ook op implantaten of met het lichaam geïntegreerde apparaten worden toegepast, omdat dit 'geautomatiseerde werken' in de zin van artikel 80sexies Sr zijn. Een officier van justitie moet een bevel daartoe afgeven en een rechter-commissaris moet dan een machtiging afgeven. Na het (mogelijk op afstand) binnendringen van het geautomatiseerde werk kan onder andere een bevel tot stelselmatige observatie worden gegeven, kunnen gegevens worden vastgelegd, en kunnen gegevens ontoegankelijk worden gemaakt (artikel 126nba lid 1 sub c, sub d en sub e Sv).

Tijdens de parlementaire behandeling van de Wet computercriminaliteit III uitten Kamerleden en senatoren hun zorgen over de mogelijkheid dat de hackbevoegdheid op *elk* geautomatiseerd werk kan worden ingezet, zoals een pacemaker. De Staatssecretaris van Veiligheid en Justitie overwoog hierover in 2016:

> "Hoewel een pacemaker onder de definitie van geautomatiseerd werk valt, zullen hierin naar verwachting geen gegevens te vinden zijn die bijdragen aan plaatsbepaling van een persoon. In de praktijk is het tevens moeilijk denkbaar dat er zich een zo zwaarwegend belang voordoet dat het door de leden van deze fractie gesuggereerde binnentreden van een pacemaker proportioneel zou worden geacht."[33]

Toch had het volgens ons beter geweest in het 'Besluit onderzoek in een geautomatiseerd werken' een verbod op te

25 Zie ook D.A.G. van Toor, *Het schuldige geheugen?* (diss. Nijmegen), Deventer: Wolters Kluwer 2017; S. Ligthart, 'Coercive Neuroimaging, Criminal Law and Privacy: A European Perspective', *JLB* 2019, 6(1); S. Rainey e.a., 'Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology?', *JLB* 2020; S.L.T.J. Ligthart, 'Neurotechnieken in het strafrecht: perspectieven op rechtsbescherming', *DD* 2021/52, p. 667-682, met verwijzing naar EHRM (GK) 4 december 2008, nr. 30562/04, 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. & Marper/VK*), par. 70-86 en EHRM 13 februari 2020, nr. 45245/15, ECLI:CE:ECHR:2020:0213JUD004524515 (*Gaughran/VK*), par. 70.

26 D.A.G. van Toor, 'Het nemo-teneturbeginsel bij digitale opsporingsbevoegdheden: oproep tot discussie over fundamentele bezinning van de normering van het opsporingsonderzoek in een digitale context', *TBS&H* 2021, nr. 2, p. 89-100, S.L.T.J. Ligthart, 'Neurotechnieken in het strafrecht: perspectieven op rechtsbescherming', *DD* 2021/52, p. 667-682 en S.L.T.J. Ligthart, 'Autonomie en privacy als rechtsgronden van het zwijgrecht en het nemo tenetur-beginsel?', *NJB* 2021/2408, p. 2660-2666.

27 Zie, o.a., G.J.M. Corstens, *Het Nederlands strafprocesrecht*, bewerkt door M.J. Borgers & T. Kooijmans, Deventer: Wolters Kluwer 2021, p. 316. Zie ook HR 9 februari 2021, ECLI:NL:HR:2021:202, r.o. 7.2, *Computerrecht* 2021/63, m.nt. D.A.G. van Toor & T. Beekhuis, *NJ* 2021/120, m.nt. J.M. Reijntjes.

28 S.L.T.J. Ligthart, 'Neurotechnieken in het strafrecht: perspectieven op rechtsbescherming', *DD* 2021/52, p. 680. Zie ook D.A.G. van Toor, *Het schuldige geheugen?* (diss. Nijmegen), Deventer: Wolters Kluwer 2017, p. 298.

29 Commissie-Koops 2018, p. 101.

30 Zie in dit kader, o.a.: D. Aono, G. Yaffe & H. Kober, 'Neuroscientific evidence in the courtroom: a review', *Cognitive Research: principles and implications* 2019, nr. 4, p. 40.

31 Dat wil zeggen misdrijven, zoals geformuleerd in artikel 67 Sv en in artikel 2 Besluit onderzoek in een geautomatiseerd werk (*Stb.* 2018, 340).

32 Dit is mogelijk gemaakt met de inwerkingtreding van artikel 126nba/126uba/126zba Sv met de Wet computercriminaliteit III, *Stb.* 2019, 67. Zie ook J.J. Oerlemans, 'De Wet computercriminaliteit III: meer handhaving op internet', *Strafblad* 2017, nr. 4, p. 350-359.

33 *Kamerstukken II* 2016/17, 34372, nr. 6, p. 32.

nemen voor de inzet van de hackbevoegdheid bij geautomatiseerde werken in het menselijk lichaam. Het hacken van een implantaat met het lichaam geïntegreerd geautomatiseerd werk brengt niet alleen een vergaande inbreuk op het recht op privacy en de lichamelijke integriteit met zich mee, maar het (onbedoeld) beïnvloeden van de werking van het implantaat kan ook gezondheidsrisico's voor de verdachte met zich meebrengen.

Wanneer het gebruik van implantaten en met het menselijk lichaam geïntegreerde apparaten zoals geavanceerde prothesen gemeengoed wordt, sluiten wij het niet uit dat zich situaties voordoen waarbij opsporingsinstanties het toch noodzakelijk vinden op afstand deze apparaten binnen te dringen om gegevens uit te lezen ten behoeve van de waarheidsvinding. Mocht de maatschappij het wenselijk achten dat de opsporing dergelijke mogelijkheden krijgt, dan is het zaak deze via een bijzondere regeling te omkleden met voldoende waarborgen.

3.4 *Traceren van apparaten in het menselijk lichaam*

Wij leven momenteel in het tijdperk van het 'internet der dingen' (*Internet of Things*), waarbij allerlei apparaten verbonden zijn met het internet.[34] Naast het 'internet der dingen' ontstaat er door draagbare apparaten (*wearables*) en implantaten langzamerhand ook een 'Internet der Mensen' (*Internet of People*). De volgende stap is dat al deze apparaten en mensen naadloos op elkaar aansluiten en met elkaar samenwerken waardoor en er een 'internet van alles' (*Internet of Everything*) ontstaat. Naast interconnectiviteit spelen ook sensoren en mens-machine interfaces een belangrijke rol in deze ontwikkeling.[35]

Een belangrijke mogelijkheid die deze ontwikkeling met zich meebrengt voor de opsporing, is dat de met het internet verbonden apparaten in het lichaam eenvoudig de locatie van personen kunnen weergeven en het mogelijk maken hen door de tijd heen te volgen. Het is denkbaar dat implantaten, bionische ledematen en mens-machine interfaces door middel van logging steevast een locatie teruggeven aan de fabrikant. Deze gegevens kunnen worden opgevraagd door opsporingsdiensten, mogelijk ook *near real time*, door 'toekomstige gegevens' te vorderen met de bijzondere opsporingsbevoegdheid in artikel 126ne Sv (in dat geval is er ook een machtiging van een rechter-commissaris noodzakelijk).

Daarnaast sluiten wij niet uit dat op een andere heimelijke manier (zoals via een hack) personen via hun apparaat gevolgd kunnen worden. Het ligt voor de hand dat daarbij dan een bevel wordt afgegeven voor toepassing van de hackbevoegdheid in combinatie met stelselmatige observatie (artikel 126nba Sv jo artikel 126g Sv). Voor het volgen van personen door middel van de inzet van de hackbevoegdheid gelden in Nederland strengere voorwaarden dan normaal. Dit is alleen mogelijk in opsporingsonderzoeken naar een misdrijf met een gevangenisstraf van acht jaren of meer, of een van de delicten (met name computerdelicten) die worden genoemd in artikel 2 van het Besluit onderzoek in geautomatiseerde werken.[36]

Net als in de voorgaande paragrafen wijzen wij erop dat het gebruik van apparaten *in* het menselijk lichaam een andere lading heeft dan apparaten *aan* het menselijk lichaam. Een apparaat in het menselijk lichaam kan namelijk niet worden afgedaan en vaak zelfs niet eens worden uitgezet. De privacy-inbreuk is groter als op die wijze personen gelokaliseerd of getraceerd worden. De wetgever moet daar volgens ons rekening mee houden als overheidsinstanties op deze wijze personen willen volgen, door het lokaliseren en traceren van apparaten in het lichaam te verbieden of dit slechts onder stringente voorwaarden mogelijk te maken.[37]

4. Conclusie

In dit artikel hebben wij de strafrechtelijke aspecten onderzocht van implantaten en met het menselijk lichaam geïntegreerde apparaten, zoals geavanceerde prothesen. De bespreking in paragraaf 2 van mogelijk toepasselijke delictsomschrijvingen laat zien dat er voor een deel is sprake is van 'old crimes with new tools', oftewel bestaande delicten worden gepleegd met behulp van nieuwe technologische middelen. Aan de genoemde strafbaarstellingen voor hacking valt op dat hoge gevangenisstraffen van toepassing zijn als het fysieke beschadiging of zelfs de dood tot gevolg heeft. Voor de reguliere computerdelicten is vaak maximaal vier jaar gevangenisstraf van toepassing en zijn slechts strafverzwaringen van toepassing als grote hoeveelheden apparaten worden aangetast, de apparaten onderdeel van een vitale infrastructuur zijn, of als de aanval kwalificeert als terroristisch misdrijf.

Het belangrijke verschil bij het type delicten dat wij hier bespreken is dat de meeste van deze delicten gericht zijn tegen apparaten *in* het menselijk lichaam in plaats van apparaten *buiten* het menselijk lichaam. Het verschil zit met name in de aantasting van de lichamelijke integriteit als wordt binnengedrongen in apparaten in het menselijk lichaam. In navolging van Gasson & Koops pleiten wij daarom voor de invoering van een hogere maximale gevangenisstraf als in apparaten *in* het menselijk lichaam wordt binnengedrongen. Dit doet recht aan de aantasting van de lichamelijke integriteit van het slachtoffer en de ernstige

34 Zie ook J. van Berkel e.a., '(Verkeerd) verbonden in een slimme samenleving', WODC 2017.
35 Commissie-Koops 2018, p. 16.
36 Daarbij tekenen wij aan dat het de vraag is of het huidige artikel 126nba Sv voor deze toepassing de ruimte biedt, omdat in artikel 126nba lid 1 sub c Sv staat dat ter uitvoering van het bevel 'een technisch hulpmiddel op een persoon *wordt bevestigd*'.
37 Zie ook eerder ook B.W. Schermer, 'High tech crime en ambient intelligence', *Computerrecht* 2010/173.

schade die daarmee gepaard kan gaan. Tegelijkertijd tekenen we daarbij aan dat het strafrecht een ultimum remedium is en een strafverzwaring slechts beperkt een bijdrage levert aan de bestrijding van deze vorm van misdaad. Juist ook het stellen van kwaliteits- en beveiligingseisen voor implantaten, bionische ledematen en mens-machine interfaces (*security-by-design*), zullen de mogelijkheden van misbruik door derden beperken.

Paragraaf 3 laat zien dat implantaten, bionische ledematen en mens-machine interfaces ook nieuwe mogelijkheden bieden voor de opsporing. Uit onze analyse van het formeel strafrecht blijkt dat die mogelijkheden er met name zijn vanwege de mogelijkheden tot het uitlezen van de apparaten in het menselijk lichaam. Wij sluiten zelfs niet uit dat gedachten kunnen worden uitgelezen als brein-machine interfaces realiteit worden. De wetgever is daarbij aan zet om duidelijk te maken welke vormen van opsporing nog een brug te ver zijn, vanwege inbreuken op fundamentele rechten zoals het recht op privacy, het zwijgrecht en zelfs de vrije wil van de verdachte.

Gegeven de vergaande inbreuk op de rechten en de autonomie van de verdachte, maar ook de mogelijke (gezondheids)-risico's die het hacken van implantaten, bionische ledematen en mens-machine interfaces met zich mee kunnen brengen, pleiten wij voor een tijdelijk verbod op het uitlezen van hersensignalen en het hacken van apparaten die in het menselijk lichaam aanwezig zijn. Andere opsporingsmethoden vinden wij minder bezwaarlijk, maar dienen wel met voldoende waarborgen omgeven te zijn, waarbij met name recht wordt gedaan aan het belang van de bescherming van de lichamelijke integriteit.

Wij roepen de Nederlandse wetgever dan ook op alsnog de door de Commissie-Koops voorgestelde schakelbepaling in het nieuwe Wetboek van Strafvordering over te nemen, zodat onderzoek aan implantaten in het lichaam slechts onder strengere voorwaarden mag plaatsvinden.