Genealogische DNA-databanken: consequenties van het delen van ons DNA

Nico Kaptein[*]

In dit artikel wordt een beeld geschetst van de consequenties van de verspreiding van DNA door burgers die buiten het medische circuit hun DNA opsturen en laten testen. Degene die het DNA instuurt, heeft veelal nauwelijks zicht op wat er vervolgens met het materiaal en met het resultaat van de analyse gebeurt. Op gegevens die door politie en justitie worden beheerd, is strikte doelbinding van toepassing, net als binnen het gereguleerde medische circuit. Private ondernemingen die DNA ontvangen van mensen die dit vrijwillig insturen ten behoeve van genealogische analyse, vallen niet onder een dergelijk regime en staan niet onder vergelijkbaar toezicht van autoriteiten. In tegenstelling tot sommige andere landen is er in Nederland geen belemmering om het eigen DNA te delen, ongeacht wat ermee gebeurt. In het publieke debat ontstaat er geleidelijk enige aandacht voor deze ontwikkeling en de risico's die hier het gevolg van zijn. Dit is nog niet vertaald in politieke keuzes en beleid.

In de afgelopen jaren is de technologie om DNA te isoleren en analyseren verder ontwikkeld. DNA-materiaal kan steeds eenvoudiger, goedkoper, sneller en met meer betrouwbaarheid worden benut voor onderzoek en analyse. DNA-technologie wordt benut voor analyse van het eigen DNA, voor opsporing en identificatie, en voor gezondheid en lifestyle. In toenemende mate speelt de analyse van DNA dat door individuele consumenten direct is opgestuurd naar commerciële aanbieders van DNA-tests hierbij een rol. Voor een overzicht van de toepassing hiervan in de opsporing en identificatie verwijs ik naar de artikelen van M'charek en De Knijff, De Poot en van Meulenbroek en Aben elders in dit themanummer.

Het doel van dit artikel is om bewustwording te stimuleren over de onomkeerbare gevolgen van de verspreiding van DNA vanwege recre-

* Drs. N. Kaptein is directeur van advies- en onderzoeksbureau Maruda.

doi: 10.5553/JV/016758502021047001006

atief gebruik en daarmee een bijdrage te leveren aan het debat. Het is geen pleidooi tegen toepassingen van DNA-technologie, maar veel meer een oproep om als samenleving bewuste afwegingen te maken, met inzicht in de risico's. In dit artikel wordt verkend wat er met DNA-gegevens gebeurt nadat deze voor recreatieve doeleinden zijn ingestuurd, hoe dit zich in de tijd heeft ontwikkeld en wat daarvan de consequenties zijn of kunnen zijn. Op basis daarvan worden aandachtspunten benoemd.

Het laten analyseren van je eigen DNA werkt als volgt: je koopt bij een commerciële aanbieder van een test een 'kit' waarmee je zelf een monster van je eigen DNA kunt nemen, bijvoorbeeld door met een wattenstaafje wat wangslijmvlies af te nemen. Het monster stuur je naar het bedrijf, waar het DNA wordt geanalyseerd. Het resultaat van de analyse is een profiel van het DNA. Het profiel wordt opgeslagen en gebruikt om informatie over afstamming en kenmerken van de persoon die het DNA heeft ingestuurd af te leiden.[1] Deze ontvangt een rapport met het resultaat van de analyse. Er zijn verschillende bedrijven die dergelijke tests laagdrempelig aanbieden.
Er zijn daarnaast verschillende voor het publiek toegankelijke databases waar het mogelijk is de resultaten van een DNA-analyse aan te bieden en te laten onderzoeken of er verwantschap is met andere personen die hetzelfde hebben gedaan. De meeste van deze databases zijn private initiatieven, zoals die van het bedrijf GEDmatch. Soms speelt de overheid een rol: in België richt de overheid een DNA-databank op waar burgers vrijwillig hun DNA kunnen afstaan ten behoeve van afstammingsonderzoek (tot in de eerste graad). Dit is een uitzondering.
Volgens opgave van de bedrijven zelf hebben per februari 2021 ongeveer 37 miljoen mensen hun DNA laten testen door de bedrijven 23andMe, AncestryDNA, FamilyTreeDNA en MyHeritage. In 2019 werd dit aantal nog geschat op 26 miljoen. Volgens sommigen groeit de markt voor DNA-tests door van € 360 miljoen in 2019 tot € 1,8 miljard in 2024. Inmiddels zijn er echter ook signalen dat de groei stagneert ten gevolge van bezorgdheid over privacy. Dit leidt paradoxaal genoeg tot verdere verspreiding van DNA-gegevens: de bedrijven gaan op zoek naar aanvullende businessmodellen (Hamzelou 2020). In de

1 Zie voor een gedetailleerde beschrijving de bijdragen van Meulenbroek en Aben en van De Poot elders in dit themanummer.

doi: 10.5553/JV/016758502021047001006

rest van dit artikel wordt toegelicht dat deze ontwikkeling risico's met zich meebrengt.

Toenemende verspreiding van DNA-gegevens

Ons DNA wordt in toenemende mate verspreid, zonder dat we daar zicht op hebben en toezicht op houden. Omdat DNA onvervreemdbaar aan onze identiteit is gekoppeld, is dit een onomkeerbaar proces. Niet alleen groeien de databases van bedrijven en organisaties die DNA ontvangen, steeds vaker wordt het DNA vervolgens ook voor andere doelen gebruikt of met andere bedrijven of organisaties gedeeld. In deze paragraaf wordt dit nader toegelicht.
Het besef groeit dat DNA-informatie commerciële waarde vertegenwoordigt. Nu een deel van de markt voor het genealogisch laten onderzoeken van het eigen DNA lijkt te stagneren, wordt de druk op bedrijven om de (eerder) ontvangen DNA-gegevens op een andere manier te gelde te maken groter: de bedrijven verdienen geld met het doorverkopen van hun gegevens.
Bedrijven combineren toepassingen van DNA steeds vaker, onder andere door overnames van andere bedrijven. Begin 2021 maakt 23andMe – in het bezit van DNA-data van meer dan 10 miljoen mensen – bekend samen met het aan Richard Branson gelieerde bedrijf VG Acquisition Corp – een zogenoemde SPAC (special purpose acquisition company) – een beursgang voor te bereiden. Dit leidt tot zorgen over de gevolgen voor de privacy van de mensen die hun DNA door 23andMe hebben laten onderzoeken. De waardering voor het bedrijf is immers gebaseerd op de DNA-gegevens waarover 23andMe beschikt, die gebruikt gaan worden voor producten op het vlak van 'digital health', geneesmiddelen en niet nader genoemde andere zaken. Op dat moment wordt 23andMe gewaardeerd op ongeveer $ 3,5 miljard. Door de overname bepalen financiële belangen wat er met de gegevens gaat gebeuren.
Op basis van DNA van gebruikers van bedrijven die DNA analyseren, ontwikkelen farmaceutische bedrijven medicatie en medische toepassingen. MyHeritage werkt bijvoorbeeld samen met *genomics*-bedrijf BGI om tests op COVID-19 te ontwikkelen. Het bedrijf 23andMe benut zijn database om – na expliciete toestemming – gegevens over besmet-

doi: 10.5553/JV/016758502021047001006

ting met SARS-COV-2 en de symptomen per individu te matchen met DNA-gegevens.
De consequentie van deze ontwikkelingen is dat DNA dat wordt ingestuurd voor een persoonlijke analyse van het eigen DNA, ook voor andere doeleinden wordt gebruikt. Er zijn grote verschillen tussen bedrijven als het gaat om het bieden van openheid en duidelijkheid hierover en in het expliciet toestemming vragen. Dit betekent dat ten gevolge van tientallen miljoenen analyses van eigen DNA steeds meer van ons DNA verspreid raakt zonder dat we zicht hebben op waar ons DNA terechtkomt en op wat er precies met dit DNA gebeurt. Omdat DNA per definitie gedeeltelijk gedeeld wordt met verwanten, raakt dit niet alleen degenen die ervoor kiezen het DNA in te sturen, maar ook hun familieleden. Familieleden wordt niet om toestemming gevraagd. Zij weten veelal niet dát hun verwant DNA heeft afgestaan, laat staan waar de DNA-gegevens terechtkomen en wat ermee gebeurt.
Niet iedereen ziet het verzamelen en verspreiden van steeds meer DNA-gegevens als een probleem: het biotechstart-up Lifeship is van plan om DNA van al het leven op aarde naar de maan te brengen en te bewaren, bij wijze van back-up van het menselijk leven (Dormehl 2019).
De bedrijven zelf doen veel moeite om de aandacht te vestigen op de kansen die het laten testen van DNA biedt en hierover een positief beeld achter te laten. Ze werken samen met andere organisaties en sponsoren evenementen. In 2019 tekende voetbalclub Ajax een contract met MyHeritage om hun 'marketing partner' te worden, waarbij werd verwezen naar kernwaarden 'innovatie' en 'diversiteit'. Ook in 2019 was MyHeritage sponsor van het Eurovisie Songfestival in Tel Aviv.

Ethische en juridische open eindes

Op het verzamelen, analyseren en delen van genetische informatie is een juridisch kader van toepassing. Niet alle sociale en maatschappelijke normen zijn in verdragen of wetten verankerd.

doi: 10.5553/JV/016758502021047001006

Juridische kaders per land verschillend

In de Nederlandse context vormen het Europees Verdrag voor de Rechten van de Mens (EVRM) en EU-Richtlijn 2016/680 het belangrijkste toetsingskader voor specifieke nationale wetgeving. De nationale wetgeving kan door het Europees Hof voor de Rechten van de Mens worden getoetst aan de genoemde Europese kaders. Ook het VN-mensenrechtencomité kan zich over een nationale wet uitspreken. Verschillende van de hier genoemde wetten zijn op enig moment getoetst aan een of meer van genoemde internationale verdragen. Wanneer in het kader van wetenschappelijk onderzoek en/of in het kader van de patiëntenzorg van een zorginstelling DNA wordt afgenomen, bewaard en/of geanalyseerd, is hierop een stevig juridisch kader van toepassing.

De kaders voor commerciële tests zijn nog relatief recent en in ontwikkeling. Tot 2017 was het zelf laten testen van DNA in de Verenigde Staten alleen toegestaan voor genealogische analyse, vanaf dan worden stap voor stap ook *direct-to-consumer* (DTC)-tests op risico's voor een aantal specifieke ernstige ziekten goedgekeurd. Er zijn in Nederland, in tegenstelling tot in sommige andere Europese landen, geen beperkingen voor burgers om hun DNA voor analyse aan private bedrijven aan te leveren. In bijvoorbeeld Frankrijk en Duitsland, waar DNA-analyse gevoelig blijft, mogen burgers hun DNA niet opsturen om dit door (internationale) bedrijven te laten analyseren, om de privacy van de burgers en de vertrouwelijkheid van de gegevens te beschermen. Desondanks hebben naar schatting een miljoen Fransen dit inmiddels toch gedaan. Er gaan dan ook stemmen op om de genealogische en gezondheidstests te reguleren in plaats van te verbieden. Dit is vooralsnog niet gebeurd.

De bedrijven die tests aanbieden, hebben in de regel een expliciet privacybeleid en sluiten met iedereen die DNA instuurt een licentieovereenkomst. Het is de vraag of mensen deze overeenkomst wel lezen voor ze deze aangaan. Wie leest immers de licentieovereenkomst van bijvoorbeeld software? De regels en afspraken zijn voorts niet waterdicht en er is nauwelijks (toe)zicht op de naleving ervan. GEDmatch heeft, na kritiek op het gebruik door de politie van haar database om de zogenoemde Golden State Killer op te sporen, haar voorwaarden gewijzigd, zodat alleen door autoriteiten gematcht mag worden na een expliciete opt-in. Bedrijven die DNA in hun database hebben, delen

doi: 10.5553/JV/016758502021047001006

dit dus niet zomaar op verzoek met opsporingsinstanties. Het bedrijf Ancestry, bijvoorbeeld, heeft in de tweede helft van 2020 naar eigen zeggen twee keer geweigerd op zo'n verzoek van autoriteiten in te gaan, waarna het verzoek werd ingetrokken.
Ook wanneer expliciet geen toestemming is gegeven, kan (tenminste in de Verenigde Staten) de politie na tussenkomst van een rechter alsnog toegang krijgen tot DNA-gegevens die zijn ingestuurd ten behoeve van een genealogische analyse. Ancestry heeft in 2019 zes keer meegewerkt aan een politieonderzoek door aan de politie DNA-gegevens te verstrekken na een gerechtelijk bevel daartoe. Het is daartoe ook wettelijk verplicht. Dit geldt ook als geen toestemming is gegeven door de verstrekker van het DNA, omdat de rechter dit al heeft meegewogen bij de beslissing tot het gerechtelijk bevel: het belang van de opsporing is in zo'n geval door de rechter als daartoe bevoegde instantie als zwaarder wegend beoordeeld dan het belang van bescherming van DNA-gegevens. In sommige staten van de Verenigde Staten (zoals in Utah[2]) wordt inmiddels wetgeving voorbereid om de politie te verbieden om gebruik te maken van private databases wanneer zij geen verdachte in beeld hebben.

Eigendom DNA onbepaald

Het is niet duidelijk van wie DNA precies is. Dit levert dan ook problemen op wanneer besluiten moeten worden genomen over wat met DNA en DNA-informatie mag worden gedaan. Tijdens het World Economic Forum in 2020 heeft een groep van deskundigen in verschillende disciplines een 'biodata bill of rights' opgesteld, met daarin het voorstel om een aantal rechten te onderkennen: het recht op eigendom van de eigen biodata, het recht op inzicht in hoe deze worden verzameld, bewaard en gedeeld, het recht op anonimiteit van biodata en het recht op 'dynamic consent', zodat voor elke toepassing specifiek toestemming gegeven wordt. De status van dit document is vooralsnog een discussiestuk: er is nog niets afgesproken.
De implicatie van deze onduidelijkheid over het eigendom van DNA is dat burgers, ondanks de bescherming van een wettelijk kader en tot op zekere hoogte door contracten en algemene voorwaarden van bedrijven, geen universele en onvervreemdbare zeggenschap hebben

2 Zie: https://www.fox13now.com/2020/01/01/police-could-be-banned-from-accessing-home-dna-test-data-under-a-bill-in-the-utah-legislature/.

doi: 10.5553/JV/016758502021047001006

over hun DNA, terwijl we de consequenties van de verspreiding van ons DNA nog onvoldoende overzien.

Informed consent niet volledig mogelijk

Een gangbaar principe bij het opslaan en gebruik van tot personen herleidbare gegevens is dat van 'informed consent'. Dit houdt in dat personen die DNA-gegevens beschikbaar stellen, zijn geïnformeerd over het gebruik ervan en daarvoor expliciet toestemming hebben gegeven. Dit beginsel geldt ook bij het gebruik van DNA-materiaal, waarbij een aantal uitzonderingen wettelijk is verankerd.
Een fundamenteel probleem hierbij is dat met het delen van het eigen DNA onvermijdelijk ook informatie over verwanten wordt gedeeld, omdat hun DNA aan het eigen DNA is gerelateerd. Verwanten worden echter niet systematisch geïnformeerd en aan verwanten wordt in het algemeen geen toestemming gevraagd. Iemand kan zelf beslissen direct familieleden te raadplegen, maar hiervoor bestaat nog geen proces, verplichting of toezicht. Er is dus geen sprake van informed consent voor een groot aantal mensen die wel traceerbaar zijn met behulp van het DNA van hun verwant. Zo worden mensen blootgesteld aan de risico's die gepaard gaan met de verspreiding van DNA, zonder dat zij hierover zelf hebben kunnen beslissen.

Consequenties, risico's en bedreigingen

Schending van privacy en persoonlijke levenssfeer

Ons DNA is – meer nog dan andere biometrische gegevens – onlosmakelijk met ons verbonden. Het delen van DNA is daarmee onomkeerbaar en kan – wanneer dit zonder toestemming gebeurt – worden beschouwd als een inbreuk op de privacy en persoonlijke levenssfeer. Ook als wel toestemming wordt gegeven, is hiervan mogelijk sprake, omdat nog niet kan worden overzien welke informatie uit het DNA in de toekomst kan worden afgeleid en hoe deze informatie gaat worden gebruikt. Wanneer ouders DNA van hun kinderen laten analyseren, weten zij niet in hoeverre dit ten koste gaat van de privacy van hun kinderen later: die verliezen daarmee feitelijk

doi: 10.5553/JV/016758502021047001006

het recht om bepaalde zaken niet te weten, terwijl geen sprake kan zijn van 'informed consent'.

Het recht om niet te weten wordt geschonden

Inzicht in ons DNA, bijvoorbeeld in relatie tot gezondheidsrisico's, kan ook onbedoelde gevolgen hebben. Het kan verplicht zijn om gezondheidsinformatie te delen met verzekeraars of geldverstrekkers, doordat dit in de meeste polissen als generieke verplichting is opgenomen. Kennis van het risico op specifieke ernstige ziekten door analyse van het eigen DNA kan worden gezien als gezondheidsinformatie, zodat deze kennis gedeeld moet worden met de betreffende verzekeraar of bank. Deze kan dan besluiten een aanvraag voor bijvoorbeeld een hypotheek of een levensverzekering af te wijzen. Wellicht worden in de toekomst nog andere controles mogelijk. Hierbij is van belang dat kennis over erfelijke belasting ook verwanten kan betreffen, inclusief kinderen en kleinkinderen die dan niet meer zelf kunnen beslissen of ze dergelijk inzicht wel willen hebben. Daarnaast kan informatie over risico's op ernstige ziekten onzekerheid en psychische belasting met zich meebrengen, terwijl de validiteit van de betreffende tests vaak nog onduidelijk is. Wetenschappers benoemen 'het recht om niet te weten' als een belangrijk principe. Het recht om niet te weten is vooralsnog niet expliciet verankerd in kaders of wetgeving.

Discriminatie

Naarmate we meer inzicht krijgen in ons DNA – en dus beter in staat zijn om zinvol onderscheid te maken tussen personen –, neemt ook het risico toe dat dit onderscheid op gespannen voet staat met het beginsel van gelijke behandeling. Dit is deels al aan de orde. DNA-analyses moeten mogelijk (door burgers zelf) worden gedeeld met verzekeraars, met consequenties voor verzekeringnemers. Personen kunnen van voorzieningen worden uitgesloten indien zij hun DNA niet afstaan. In Florida is een wet in de maak om te verbieden dat een verzekering wordt beperkt of beëindigd op basis van DNA-gegevens. Wanneer medewerkers van het ministerie van Defensie in de Verenigde Staten hun DNA laten testen, kan dit ten koste gaan van hun carrièrekansen, omdat zij niet worden beschermd door de desbetreffende wetgeving (GINA, de Genetic Information Nondiscrimina-

doi: 10.5553/JV/016758502021047001006

tion Act). Ook de staat Florida waarschuwt zijn burgers voor dergelijke consequenties van het laten testen van hun DNA.
Een ander risico is dat bij de verdeling van middelen onder druk onderscheid wordt gemaakt op basis van informatie over iemand die is ontleend aan diens DNA. Zo'n scenario zou zich kunnen voordoen wanneer bij een epidemie schaarste aan IC-bedden ontstaat en een keuze gemaakt moet worden aan wie zorg wordt verleend, maar ook bijvoorbeeld bij investering in opleiding of bij werving en selectie (Thibodeau 2016). Dit is voor zover bekend nog niet aan de orde – en op basis van de stand van kennis vooralsnog ook niet zinvol. Ook hierbij geldt: mogelijk is dit in de toekomst anders. Als iemands DNA dan al verspreid is en er hierover geen controle is, is daar tegen die tijd mogelijk niets meer aan te doen.
Etnische groepen zijn niet evenwichtig vertegenwoordigd in DNA-databanken, zodat inzicht uit DNA-onderzoek op sommige groepen meer zal zijn toegesneden dan op andere. Dit betreft onder andere 'precision medicine', de belofte dat artsen op basis van het DNA van een patiënt de beste passende behandeling en medicatie bepalen. Ook binnen etnische groepen zijn er verschillen naar leeftijd, geslacht en/of sociale achtergrond in de mate waarin DNA is vertegenwoordigd in de databanken. Ook oververtegenwoordiging van etnische groepen in de DNA-databanken, zoals ten gevolge van het afnemen van DNA van immigranten in de Verenigde Staten, kan tot ongelijke behandeling leiden. Een ander voorbeeld is het verwijt aan China ten aanzien van het gericht verzamelen van het DNA van Oeigoeren. Al met al brengt de verspreiding van DNA tot dusverre met zich mee dat kansen en risico's voor verschillende etnische groepen verschillend uitpakken, met het risico op discriminatie.

Informatieveiligheid

Net zoals bij andere typen gegevens kan de integriteit van DNA-gegevens worden aangetast. DNA-materiaal kan worden besmet, waardoor een eventuele match incorrect kan worden geïnterpreteerd. Soms is DNA-materiaal al gemengd en/of besmet wanneer het wordt veiliggesteld.
Daarnaast zijn ook de klassieke informatieveiligheidsrisico's van toepassing. In de Verenigde Staten zijn voorbeelden bekend van phishing van DNA-materiaal door zogenaamd een gratis DNA-analyse

doi: 10.5553/JV/016758502021047001006

aan te bieden (Perez 2019), waarna onduidelijk is wat er met het DNA gebeurt. Actueel is een voorbeeld waarbij zogenaamd een gratis test op COVID-19 wordt aangeboden. DNA-databanken kunnen worden gehackt (Vaughan 2019), bijvoorbeeld door vreemde mogendheden. Soms gaat het daarbij alleen om persoonsgegevens en niet om het DNA zelf. Ook DNA-gegevens kunnen worden onttrokken aan bestanden, bijvoorbeeld door kwetsbaarheden in genetische-genealogiewebsites. DNA-materiaal kan bovendien per ongeluk worden vernietigd. Naarmate er minder zicht is op hoe DNA-gegevens worden verzameld, bewaard, beveiligd, gedeeld en/of geanalyseerd, is niet duidelijk welke risico's aan de orde zijn. De gevolgen van de ongecontroleerde verspreiding voor de informatieveiligheid zijn onzeker, maar het is te verwachten dat er op een zeker moment ongewenste effecten naar boven zullen komen.

Risico's voor de nationale veiligheid

In de meest recente Geïntegreerde risicoanalyse Nationale Veiligheid (Analistennetwerk Nationale Veiligheid 2019) komt het woord DNA (nog) niet voor. In het buitenland wordt de verspreiding van DNA echter steeds meer als een risico voor nationale veiligheid gezien. De kennis en methoden om DNA te manipuleren kunnen worden gebruikt om virussen aan te passen in het kader van biologische oorlogvoering (Menachery e.a. 2015). In reactie op de zichtbare impact van COVID-19 is aan dit risico aandacht besteed, al zijn er geen concrete aanwijzingen dat dit daadwerkelijk gebeurt. Wetenschappers houden met betrekking tot COVID-19 de mogelijkheid open van een lek bij het Chinese Centrum voor Infectieziektebeheersing en Preventie in Wuhan en/of het Wuhan Virologie Instituut, maar gaan vooralsnog niet uit van een bewuste actie of van een biologisch wapen. De Verenigde Staten beschuldigen China ervan DNA te verzamelen zodat het zowel zijn eigen burgers als individuen uit andere landen kan 'targeten', onder wie specifiek buitenlandse spionnen. De Amerikaanse inlichtingendienst NCSC (National Cyber Security Center) heeft in februari 2021 een factsheet gepubliceerd waarin wordt aangegeven op welke wijze vanuit China 'legaal en illegaal' toegang zou zijn verkregen tot gezondheidsgegevens van Amerikaanse burgers, waaronder informatie over hun DNA. De veiligheidsmaatregelen met

doi: 10.5553/JV/016758502021047001006

betrekking tot de toegang tot DNA in de Verenigde Staten zijn gericht op privacy, niet op nationale veiligheid.
Zo hebben Chinese bedrijven belangen genomen in Amerikaanse bedrijven die toegang hebben tot gevoelige gezondheidsgegevens, zoals Complete Genomics en Nextcode Health. Daarnaast werken Chinese bedrijven samen met Amerikaanse ziekenhuizen, universiteiten en onderzoeksinstellingen. Het Amerikaanse NCSC wijst erop dat Chinese bedrijven onder de Chinese wet verplicht zijn om gegevens met de overheid te delen. Bovendien suggereert het genoemde factsheet dat Chinese organisaties ook langs illegale weg toegang krijgen tot (Amerikaanse) medische gegevens, waaronder gegevens uit DNA-databanken. Dit zou met name via cyberaanvallen gebeuren.
Dergelijke risico's hebben vermoedelijk ook betrekking op andere landen, mogelijk als 'verzamelaar' van DNA-gegevens en ten minste als beheerder van DNA-databanken. Hier dient te worden aangetekend dat Europese regels (en het toezicht daarop) mogelijk meer bescherming bieden dan de Amerikaanse, en zeker meer dan de regels in veel andere landen.
In Nederland is soms ook sprake van nauwe banden met Chinese onderzoekers of bedrijven. In 2019 kwam het Erasmus MC in het nieuws naar aanleiding van een bericht in *The New York Times* dat een Chinese docent van het Erasmus MC eveneens werkzaam was bij het Beijing Institute of Genomics. Deze docent bleek coauteur te zijn van een studie naar het DNA van Oeigoeren. Dit ligt gevoelig, omdat het vermoeden bestaat dat DNA-technologie wordt gebruikt bij de onderdrukking van Oeigoeren in China.

Risico's voor de rechtsstaat

Op verschillende manieren kan het toenemend toepassen van DNA-technologie een bedreiging vormen voor het correct en rechtmatig verloop van strafzaken. Advocaten en rechters kunnen, mede vanwege de complexiteit van de bewijsvoering, fouten maken bij zaken waarbij DNA-bewijs een rol speelt. Na beenmergtransplantaties kan vreemd DNA tot (initieel) incorrecte identificatie leiden. Er is bij deskundigen voldoende kennis op dit vlak, maar dat betekent niet dat deze kennis bij specifieke strafzaken altijd beschikbaar is en wordt benut. Daarnaast is er het risico van eigenrichting. Eigenrichting kan plaatsvinden door een DNA-sample van een onbekende persoon te verkrijgen en in

doi: 10.5553/JV/016758502021047001006

te sturen met als doel om de bronpersoon van het DNA te identificeren, bijvoorbeeld na een inbraak of een zedenmisdrijf. Ook kan sprake zijn van eigenstandig optreden nadat overspel wordt aangetoond aan de hand van een 'infidelity test'. Ten slotte kan sprake zijn van identiteitsfraude. Identiteitsfraude kan bijvoorbeeld plaatsvinden door het DNA van iemand anders af te staan alsof het eigen DNA betreft.

Conclusie

Het overzicht van ontwikkelingen en risico's geeft het beeld dat waar het gebruik van DNA in de opsporing en binnen de reguliere gezondheidszorg in belangrijke mate geregeld en geborgd is, dit niet geldt voor de risico's met betrekking tot de verspreiding van DNA-informatie via genealogische databanken. Er zijn geen aanwijzingen dat de snelheid van ontwikkelingen op korte termijn afneemt, terwijl de kennis, het bewustzijn en dus ook het beleid al achterlopen: er is weinig zicht en toezicht op de verzameling en het gebruik van DNA-gegevens. Hoewel we de risico's nog niet volledig kunnen overzien, is al wel duidelijk dat het om reële risico's gaat met potentieel grote impact. Het pleidooi is dan ook om te investeren in kennis en bewustzijn, als basis voor een debat met gelijkwaardige aandacht voor kansen en risico's. Alleen dan hebben we de kans om zélf de balans te bepalen tussen de opbrengst en de risico's van DNA-technologie.

Literatuur

Analistennetwerk Nationale Veiligheid 2019
Analistennetwerk Nationale Veiligheid, *Geïntegreerde risicoanalyse Nationale Veiligheid*, Den Haag: NCTV 2019, www.nctv.nl/documenten/publicaties/2019/6/07/geintegreerde-risicoanalyse-nationale-veiligheid.

Dormehl 2019
L. Dormehl, 'This biotech startup wants to put your DNA in a vault on the moon', *Digitaltrends.com* 17 september 2019, www.digitaltrends.com/cool-tech/lifeship-dna-archive-on-the-moon/#:~:text=The%20San%20Francisco%2Dbased%20startup,%2499%20swab%2Dbased%20DNA%20kit.

doi: 10.5553/JV/016758502021047001006

Hamzelou 2020
J. Hamzelou, 'DNA firms are set to profit from your data as testing demand falls', *New Scientist* 7 februari 2020, www.newscientist.com/article/2232770-dna-firms-are-set-to-profit-from-your-data-as-testing-demand-falls/.

Menachery e.a. 2015
V.D. Menachery, B.L. Yount, K. Debbink, S. Agnihothram e.a., 'A SARS-like cluster of circulating bat coronaviruses shows potential for human emergence', *Nature Medicine* (21) 2015, afl. 12, p. 1508-1513, www.nature.com/articles/nm.3985.pdf.

Perez 2019
J. Perez, 'Don't fall for this dna scam', *KimKomando* 23 juli 2019, www.komando.com/happening-now/582683/dont-fall-for-this-dna-scam.

Thibodeau 2016
P. Thibodeau, 'DNA testing for jobs may be on its way, warns Gartner', *Computerworld* 19 oktober 2016, www.computerworld.com/article/3132477/dna-testing-for-jobs-may-be-on-its-way-warns-gartner.html.

Vaughan 2019
A. Vaughan, 'Genetic privacy attack could reveal DNA secrets from genealogy sites', *New Scientist* 24 oktober 2019, www.newscientist.com/article/2221138-genetic-privacy-attack-could-reveal-dna-secrets-from-genealogy-sites/.

doi: 10.5553/JV/016758502021047001006