Rathenau Instituut

Ministerie van Justitie en Veiligheid
T.a.v. de Minister voor Rechtsbescherming, drs. S. Dekker
Postbus 20301
2500 EH DEN HAAG

Ons kenmerk	Uw brief van	Doorkiesnummer
2020-0783	-	070 – 342 15 42

Onderwerp reactie op Verzamelwet gegevensbescherming

Den Haag, 14 juli 2020

Geachte heer Dekker,

Met belangstelling heeft het Rathenau Instituut kennisgenomen van het op www.internetconsultatie.nl gepubliceerde concept voor het voorstel van de Verzamelwet gegevensbescherming die onder meer beoogt de Uitvoeringswet Gegevensbescherming (UAVG) te wijzigen. Graag maken wij gebruik van de mogelijkheid om op dit voorstel te reageren.

In het bijgevoegde document schetsen wij technologieën waarmee drie soorten intieme gegevens worden verzameld: genetische gegevens, biometrische gegevens en gezondheidsgegevens. We signaleren dat verwerking van deze gegevens ongewenste invloed heeft op rechten en belangen van mensen. De UAVG regelt dit op een aantal punten onvoldoende. Onze reactie biedt oplossingsrichtingen voor deze knelpunten in de UAVG.

Vorig jaar gaf het kabinet aan het wenselijk te vinden om bij nieuwe technologische ontwikkelingen systematisch na te denken over de risico's die deze technieken voor de privacy hebben.

Het is goed dat het kabinet kwesties als privacy zal agenderen, maar de tijd is inmiddels rijp voor reguleren. De technische ontwikkelingen en maatschappelijke opvattingen dwingen hiertoe. De UAVG biedt kansen om de verwerking van genetische gegevens en biometrische gegevens te reguleren. Met betrekking tot de omgang met gezondheidsgegevens kan het nodige worden verduidelijkt in de UAVG.

Wij hopen dat u onze reactie en oplossingsrichtingen in overweging neemt. Uiteraard zijn wij te allen tijde bereid om deze nader toe te lichten.

Met vriendelijke groet,

Dr. ir. Melanie Peters
Directeur Rathenau Instituut

Rathenau Instituut

Reactie Verzamelwet gegevensbescherming

Samenvatting

De overheid hoort ernaar te streven dat onze samenleving zoveel mogelijk kan profiteren van succesvolle innovatie. Daartoe moeten de kansen die nieuwe technologie biedt, zoals digitalisering, worden gegrepen. Tegelijkertijd moeten burgers zoveel mogelijk worden beschermd tegen de risico's van technologie.

De Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) dient, net als elke andere wet, relevant en toepasbaar te blijven bij nieuwe technologische ontwikkelingen. Technologieneutrale formuleringen in de wettekst helpen daarbij. Wetgeving moet worden aangepast als de wet de maatschappelijke opvattingen niet meer goed weerspiegelt. Bijvoorbeeld vanwege veranderingen in de interactie tussen maatschappij en technologie. Het Rathenau Instituut onderzoekt sociotechnische ontwikkelingen en de invloed die daaraan gerelateerde wetgeving en bestuur hebben op mensenrechten en belangen. In deze reactie schetsen we technologieën waarmee drie soorten 'intieme' gegevens worden verzameld: genetische gegevens, biometrische gegevens en gezondheidsgegevens. We leggen enkele knelpunten bloot die de UAVG niet goed regelt.

Oplossingsrichtingen zijn:

1. Verbied de verwerking van genetische gegevens door commerciële analysebureaus en door werkgevers of, als er niet tot een verbod wordt overgegaan, scherp de regels aan voor de omgang met genetische gegevens;
2. Verbied de verwerking van biometrische gegevens in de publieke ruimte en voer voor overige gevallen een vergunningsplicht in;
3. Maak duidelijk wat de voorwaarden zijn voor de verwerking van gezondheidsgegevens in het medische domein (WGBO) en daarbuiten (UAVG) en geef aan welke persoonsgegevens door een hulpverlener verwerkt mogen worden in het kader van een 'goede behandeling of verzorging c.q. beheer van de beroepspraktijk'.

Introductie: de intiem-technologische revolutie

Sinds 2012 observeren we twee trends: biologie wordt steeds meer technologie én vice versa. Levende organismen, zoals het menselijk lichaam, worden gezien als meetbare, analyseerbare en maakbare objecten. Bijvoorbeeld door het uitlezen van ons DNA, emotieherkenningstechnologie en *quantified-self*-toepassingen zoals een hardloop-app. Tegelijkertijd laten technologieontwikkelaars zich inspireren door inzichten uit de levenswetenschappen. Zo tracht het Europese *The Human Brain Project* de werking van het brein te simuleren in hard- en software. Technologie wordt steeds meer biologie, als ingenieurs de typische kwaliteiten van levende wezens als de mens in

technologie proberen in te bouwen. Door de twee trends versmelten mens en technologie met elkaar.

Deze intiem-technologische revolutie leidt tot digitalisering van de biologische wereld. Gedigitaliseerde, intieme gegevens zoals genetische gegevens, biometrische gegevens en gezondheidsgegevens, kunnen in allerlei innovaties worden toegepast. Bijvoorbeeld *artificial-intelligence(machine learning*)-toepassingen, robots of *internet-of-things*-technologie.

Hoewel deze digitale gegevens reeds decennia worden geregistreerd, signaleren we dat de manieren toenemen waarop deze gegevens worden verwerkt, de inzichten die eruit verkregen worden veelzijdiger zijn en de kosten voor het gebruik ervan steeds lager worden. Dit heeft gevolgen, zoals we zullen toelichten, op de mens en zijn fundamentele rechten en belangen. De wetgever kan deze gevolgen naar onze mening niet negeren.

1 Datatechnologieën met gevolgen voor rechten en belangen van mensen

1.1 Genetische gegevens

Artikel 28 van de UAVG gaat over genetische gegevens. Volgens de AVG zijn dit gegevens met betrekking tot overgeërfde of verworven genetische kenmerken van een persoon. Die genetische kenmerken blijken uit een analyse van een biologisch monster, zoals bloed of wangslijm. Door toepassing van bijvoorbeeld chromosoomanalyse, DNA-analyse of analyse van ribonucleïnezuur (RNA) kan uit het monster genetische informatie worden verkregen.

De voorgestelde wijziging van de UAVG beoogt geen inhoudelijke wijzigingen ten opzichte van de Wet bescherming persoonsgegevens (Wbp) uit 2001. Maar de technologie heeft sinds 2001 niet stilgestaan: anno 2020 is het uitlezen van data uit DNA veel volledi ger, gedetailleerder, sneller en goedkoper dan twintig jaar geleden dankzij nieuwe technieken als *next generation sequencing*. Ook kunnen genetische gegevens gemakkelijker worden opgeslagen en gedeeld, en kunnen er complexere en diepere analyses worden gedaan. Tijdens de totstandkoming van de Wbp kon al op basis van genetische informatie de oorzaak van een ziektebeeld worden gevonden of het risico op het krijgen van (erfelijke) ziektes later in het leven worden geschat. Tegenwoordig wordt het steeds gemakkelijker om andere inzichten te verkrijgen, onder meer omdat het menselijk DNA in de afgelopen jaren volledig digitaal in kaart is gebracht. Zo zijn er dienstverleners die stellen dat genetische gegevens inzicht kunnen geven over de etnische oorsprong van een persoon, zijn of haar persoonlijkheidstype, talenten of zelfs de mate van intelligentie.[i] De betrouwbaarheid van dit soort claims is onderwerp van discussie. Ook kunnen gegevens over iemands DNA worden gebruikt om een digitale inschatting te maken van zijn of haar gezicht, maar dit wordt in de praktijk nog niet toegepast.[ii] Hoe goed de werkelijkheid kan worden benaderd is nog onduidelijk. Er liggen nog tal van andere, mogelijke toepassingen met genetische gegevens in het verschiet, zij het met onzekerheden en beperkingen.

Tijdens de totstandkoming van de Wbp werden genetische gegevens vooral gebruikt in het medische domein, voor wetenschappelijk onderzoek of in het forensische domein ten behoeve van opsporing of bewijsvoering in het strafproces. Hoewel die domeinen nog steeds relevant zijn, richten we ons hier op twee domeinen die destijds niet bestonden of waarin de genetische gegevens nauwelijks werden gebruikt. Het gaat om verwerking van genetische gegevens door commerciële aanbieders van *direct-to-consumer*-DNA-analyses (paragraaf 1.1.1) en door werkgevers (paragraaf 1.1.2). Voor beide domeinen beschrijven we hieronder enkele knelpunten.

1.1.1 Commerciële DNA-analyses: overweeg verbod of scherp voorwaarden aan

Consumenten kunnen sinds 2006 met behulp van commerciële analysebureaus als 23andMe inzicht verkrijgen in hun eigen genetisch profiel. Aanbieders claimen dat de etnische oorsprong kan worden ontdekt, een persoonlijk voedingsprofiel kan worden opgesteld,[iii] en inzicht kan worden verkregen in erfelijke aanleg voor aandoeningen en eigenschappen zoals blindheid of kaalheid.[iv] Deze gegevens zijn zeer gevoelig en dragen een hoog risico in zich voor schending van de privacy van personen. Niet alleen de privacy van degene die de test aanvraagt, maar ook van zijn verwanten.[v] Erfelijkheidsgegevens hebben per definitie betrekking op mensen die genetisch verwant zijn.

De UAVG staat het niet toe dat genetische gegevens worden verwerkt van verwanten, behalve in het geval van een zwaarwegend geneeskundig belang of wetenschappelijk onderzoek. We mogen er niet blind op vertrouwen dat de, veelal internationale, aanbieders van DNA-tests zich aan de strenge UAVG-voorwaarden houden. Een studie uit 2016 concludeerde dat een derde van de onderzochte aanbieders niet helder communiceert over de gegevensverwerkingen.[vi] Onderzoeken van de NOS in 2019 en de Consumentenbond in 2020 trekken vergelijkbare conclusies.[vii] Een ander probleem is dat de aanbieders niet met zekerheid kunnen nagaan of de genetische gegevens betrekking hebben op de aanvrager van de test. Het is niet uit te sluiten dat iemand een biologisch monster instuurt van een ander.

Worden mensen voldoende beschermd tegen de risico's? DNA is uniek en onherroepelijk. Zowel het monster als de genetische gegevens kunnen lang worden bewaard. De mogelijkheden om nadere inzichten te verkrijgen nemen mettertijd toe, waardoor nieuwe risico's voor het individu ontstaan. Op een dag kunnen de inzichten in het nadeel van de betreffende persoon worden gebruikt.

In Duitsland en Frankrijk zijn *direct-to-consumer*-DNA-analyses praktisch verboden, omdat zulke analyses alleen mogen plaatsvinden onder de begeleiding van medisch beroepsbeoefenaren.[viii] De Nederlandse wetgever kan een vergelijkbaar *de facto* verbod overwegen. Als alternatief dient de UAVG op zijn minst te verduidelijken wanneer de gegevensverwerkingen mogen plaatsvinden op basis van uitdrukkelijke toestemming[ix] en hoe er omgesprongen moet worden met de rechten van anderen, zoals verwanten in de genetische lijn. Bijvoorbeeld door eisen op te stellen die voorkomen dat aanvragers van *direct-to-consumer*-tests monsters van anderen insturen.

1.1.2 Arbeidsdomein: sta verwerking alleen toe op basis van wettelijk voorschrift

De verwerking van genetische gegevens speelt ook in het arbeidsdomein. Werkgevers willen weten of sollicitanten of werknemers geschikt zijn. Om hierachter te komen laten sommige werkgevers DNA-tests uitvoeren door commerciële bureaus, die vrijwillig benaderd kunnen worden door werknemers op suggestie van de werkgever. De werkgever hoopt met de tests (erfelijke) persoonlijkheidseigenschappen te ontrafelen van zijn (toekomstige) werknemers. Al in 2004 waarschuwden de EU-privacytoezichthouders voor dit soort tests, omdat de betrouwbaarheid ervan discutabel is en ze het ontoelaatbaar vinden dat werkenden gediscrimineerd worden op basis van genetische informatie die in de meeste gevallen een lage voorspellende waarde heeft.[x] Volgens hen zou de verwerking van genetische gegevens in de arbeidsverhouding in principe verboden moeten worden. Meer recent toonden diverse wetenschappers zich eveneens kritisch.[xi]

Ondanks de kritiek worden de tests wel uitgevoerd. Dit opent de deur naar ongerechtvaardigde discriminatie van bijvoorbeeld sollicitanten. Op basis van de DNA-analyses zouden bepaalde erfelijke eigenschappen hen minder aantrekkelijk kunnen maken voor de baan. De huidige wettekst van de UAVG mist echter verplichte maatregelen tegen de risico's van ongewenste en ongeoorloofde verwerkingen van genetische gegevens in de arbeidsverhouding. Dit terwijl de AVG daarvoor wel de ruimte biedt. Aangezien toestemming in een relatie tussen werkgever en werknemer gewoonlijk niet vrijelijk kan worden gegeven, zoals de AVG dat vereist, ligt het voor de hand dat de UAVG de verwerking van genetische gegevens van werknemers en sollicitanten alleen toestaat op basis van een wettelijk voorschrift.[xii] Het voorschrift dient onder meer zo specifiek mogelijk te beschrijven wanneer verwerking van genetische gegevens mag plaatsvinden, voor welke doeleinden en onder welke voorwaarden.

1.2 Biometrische gegevens

Artikel 29 van de UAVG reguleert de omgang met biometrische gegevens. Het zijn gegevens die verzameld worden met biometrische, steeds meer geavanceerde technologie. Oftewel: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of aan gedrag gerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd.

Er zijn allerlei biometrische technieken waarmee mensen geïdentificeerd kunnen worden. Bekende toepassingen zijn herkenning op basis van het gezicht of vingerafdrukken.[xiii] Maar identificatie is ook mogelijk op basis van onze oorschelpen, ademhaling, hartslag en houding, en ons looppatroon en stemgeluid. Ook zijn we te identificeren op basis van de manier waarop we typen.[xiv]

Het Rathenau Instituut constateerde al dat er – met uitzondering van de aandacht voor biometrische toepassingen in paspoorten – betrekkelijk weinig aandacht is voor biometrische ontwikkelingen.[xv] Dat is onterecht, gelet op de toepassingen op het vlak van gezichtsherkenning die zich in snel tempo ontwikkelen. Ten eerste staat

gezichtsherkenningstechnologie niet op zichzelf. Het wordt vaak gecombineerd met andere manieren van biometrische identificatie, zoals het (op)meten van de iris, de handpalm, het oor, het looppatroon, de ademhaling of de hartslag. Of het in kaart brengen van de textuur van de huid, het bloedvatenpatroon, de zweetporiepatronen op de vingers of door lichaamsgeurdetectie. Door deze verschillende kenmerken te combineren, lukt het steeds vaker om iemand te identificeren.

Ten tweede hebben mensen steeds minder, of soms zelfs geen, controle over de situatie waarin zij worden onderworpen aan biometrische toepassingen. Dat komt omdat veel van de toepassingen mensen van steeds grotere afstanden kunnen herkennen. Er zijn bijvoorbeeld commerciële toepassingen die mensen van meer dan 15 meter afstand kunnen herkennen[xvi] en het Amerikaanse leger ontwikkelt biometrische technologie die mensen herkent van meer dan 1 kilometer afstand.[xvii] Daarnaast kan biometrische technologie verborgen worden. Bijvoorbeeld in paspoppen van winkeletalages.[xviii]

Biometrische toepassingen zijn zeer risicovol voor de rechten en vrijheden van mensen. Elementen zoals foto's die voor een bepaald doel zijn verzameld, bijvoorbeeld voor het gebruik op sociale media, kunnen tegenwoordig voor gezichtsherkenning worden gebruikt zonder medeweten van degene die op de foto staat. Het recente voorbeeld van ClearView AI toont dit aan. Dit in Amerika gevestigde bedrijf verzamelde meer dan 3 miljard foto's van websites als Facebook en YouTube met daarop gezichten van personen. Gebruikers van de ClearView AI-app kunnen een eigen afbeelding uploaden en deze via gezichtsherkenning laten *matchen* met de verzamelde foto's. Zo kunnen gebruikers mensen identificeren voor eigen motieven zoals stalking[xix] of opsporing,[xx] terwijl de foto's destijds voor andere doelen online zijn geplaatst. Doelverschuiving (*function creep*) ligt op de loer.

Verder is de vrees reëel dat biometrische toepassingen zoals gezichtsherkenning ervoor zorgen dat iemand nooit meer anoniem kan zijn. We kunnen ons immers niet aan biometrie onttrekken, zeker niet in de publieke ruimte. Er is weinig fantasie voor nodig om vast te stellen dat biometrische technologie en andere vormen van herkenningssystemen privacy en anonimiteit onder druk zetten alsook een *chilling effect* hebben. Bijvoorbeeld op de bewegingsvrijheid van burgers en de vrijheid om te demonstreren.[xxi] Wij beschrijven hieronder aandachtspunten voor biometrie in publieke en niet-publieke ruimten.

1.2.1 Publieke ruimte: voer verbod in op biometrische toepassing

Uit de Memorie van Toelichting van de UAVG blijkt dat de wetgever in de context van artikel 29 UAVG nauwelijks acht slaat op de fundamentele rechten en belangen van burgers, maar zich vooral zorgen maakt over de situatie waarin 'bestaande ontwikkelingen in het gebruik van biometrie als identificatiemiddel sterk gehinderd zouden worden'. Bij het opsporen en voorkomen van criminaliteit, en het controleren van immigratie met biometrie, zijn rechten en belangen van burgers echter in het gedrang gekomen.

Gelet op de grote risico's voor de mensenrechten en de democratische samenleving, ligt het voor de hand dat de wetgever uiterst terughoudend is in het toestaan van

biometrische toepassingen door private en publieke partijen. Biometrische toepassingen kunnen aan de ene kant nuttig zijn als zij worden ingezet met respect voor privacy en principes als dataminimalisatie, bijvoorbeeld om na te gaan of iemand oud genoeg is om alcohol te kopen. Maar aan de andere kant kunnen de gegevens buiten het medeweten van mensen om worden verwerkt voor identificatie, ongezien en op afstand, en voor het verkrijgen van inzichten die tot discriminatie of manipulatie van individuen kunnen leiden. Vanwege deze redenen heeft het Rathenau Instituut gepleit voor het recht van burgers om niet structureel heimelijk gesurveilleerd te worden of heimelijk beïnvloed te worden, bijvoorbeeld met behulp van biometrische toepassingen.[xxii] Het kabinet heeft erkend dat dit recht reeds besloten ligt in artikel 10 van de Grondwet en artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM).[xxiii] In dit licht dient de wetgever te beoordelen of biometrische toepassingen in de publieke ruimte wel wenselijk zijn in een samenleving als Nederland.

Gelet op de risico's en de nadelige gevolgen voor de samenleving ligt een verbod, al dan niet tijdelijk, op de inzet van biometrische toepassingen in de publieke ruimte het meest voor de hand. In hun reacties op de *white paper* van de Europese Commissie over AI,[xxiv] pleiten zowel de Raad van Europa[xxv] als de EU-toezichthouder EDPS[xxvi] voor een verbod op biometrische toepassingen in de publieke ruimte, in elk geval totdat er een publiek debat is gevoerd en op EU-niveau regels zijn vastgesteld. Om dit verbod te concretiseren kan de wetgever een link leggen met de Wet openbare manifestaties (Wom). Hieronder vallen ook gemeenschappelijke ruimten zoals wegen en paden in winkelcentra. Steden als San Francisco en Boston hebben met betrekking tot gezichtsherkenning een vergelijkbaar verbod uitgevaardigd. België is eveneens kritisch.[xxvii]

Een wettelijk verbod is gelegitimeerd, omdat de door wetgever geïntroduceerde maatstaf "redenen van zwaarwegend algemeen belang" voor verwerkingsverantwoordelijken veel te vaag is. Het is namelijk niet duidelijk wat de maatstaf betekent.[xxviii] Daarnaast past een verbod in de tijdsgeest. Uit recent onderzoek blijkt dat maar 6% van de Nederlandse ondervraagden bereid was aan private partijen gegevens over zijn of haar gezicht te verstrekken voor identificatiedoeleinden. Slechts 24% wilde dat doen als het identificatie door de overheid betrof.[xxix]

1.2.2 Niet-publieke ruimte: overweeg een vergunningsplicht

Los van de te verbieden biometrische toepassingen in de publieke ruimte, is het denkbaar dat biometrische gegevensverwerking soms noodzakelijk en gerechtvaardigd is. Bijvoorbeeld voor de toegangsbeveiliging van een kerncentrale, zoals genoemd in de toelichting bij de UAVG. Er zijn ook voorbeelden waarin de noodzaak voor de biometrische toepassing minder urgent is. Zo willen houders van stadions, casino's en supermarkten gezichtsherkenning toepassen om ongenode gasten te herkennen en weren.[xxx]

Voor alle situaties die niet onder de publiek ruimte vallen, dienen de verwerkingsverantwoordelijke stadion- en casinohouders, winkeliers, etc. een vergunning te verkrijgen voordat zij de biometrische gegevens mogen verwerken. De Autoriteit Persoonsgegevens kan deze vergunning verzorgen, zoals de toezichthouder dat al doet met betrekking tot bepaalde verwerkingen van strafrechtelijke gegevens.[xxxi]

Op deze manier houdt de Autoriteit Persoonsgegevens vinger aan de pols. Bijvoorbeeld door het verbinden van voorwaarden aan de vergunning met het oog op de bescherming van de persoonlijke levenssfeer van betrokkenen.

Zonder een vergunning zouden er geen biometrische gegevens verwerkt mogen worden. Hoewel theoretisch de mogelijkheid bestaat om de gegevens te verwerken op basis van (uitdrukkelijke) toestemming, is dat niet wenselijk. Immers, kunnen mensen die toestemming werkelijk weigeren? Dat zal niet snel gebeuren. Migranten,[xxxii] werknemers[xxxiii] of leerlingen[xxxiv] bijvoorbeeld staan onder druk om toestemming te geven, omdat zij anders de landsgrens niet mogen passeren, of hun kantoor of school niet mogen betreden. In zulke gevallen voldoet de toestemming niet aan de AVG-eisen, omdat deze niet 'vrijelijk' gegeven wordt. De UAVG zou deze optie dan ook niet moeten bieden voor de verwerking van biometrische gegevens, maar de rechtsgronden beperken tot wettelijke voorschriften in combinatie met een vergunning.

1.3 Gezondheidsgegevens

Artikel 30 van de UAVG beschrijft wanneer het verbod kan worden opgeheven om gezondheidsgegevens te verwerken. Inhoudelijk is de bepaling vrijwel gelijk aan zijn Wbp-voorganger. De term "gezondheidsgegevens" moet hier breed worden opgevat.[xxxv] Het gaat om alle persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijk persoon. Hieronder vallen ook gegevens over verleende gezondheidsdiensten waarmee informatie over de gezondheidstoestand wordt gegeven.[xxxvi] Het gaat niet alleen om informatie over iemands gezondheidstoestand in het verleden en het heden, maar ook over toekomstige ziekterisico's. Patiëntnummers of andere cijfers, symbolen of kenmerken die als uniek identificatiemiddel in de gezondheidszorg worden gebruikt zijn eveneens gezondheidsgegevens. Gezondheidsgegevens zijn ook gegevens in het medisch dossier over bijvoorbeeld diagnosen, onderzoeksresultaten, beoordelingen en verrichte behandelingen of ingrepen.

Het Rathenau Instituut constateert dat consumenten en bedrijven steeds meer gezondheidsgegevens verwerken buiten de door het beroepsgeheim beschermde institutionele context die bestaat wanneer een patiënt en een hulpverlener een behandelrelatie hebben. Bijvoorbeeld via *smart wearables* waarbij een persoon zelf besluit gegevens te laten verzamelen door een apparaat en deze deelt met de aanbieder. Zulke instrumenten genereren gegevens zoals hartslag, ademhalingsfrequentie, lichaamstemperatuur en voedings- en slaappatronen. Zijn deze gegevens verzameld in het kader van een behandelrelatie, dan worden zij niet alleen beschermd door de (U)AVG, maar ook door het medisch beroepsgeheim. Het beroepsgeheim wordt onder meer uitgekristalliseerd in afdeling 5 van Titel 7 van Boek 7 van het Burgerlijk Wetboek inzake de geneeskundige behandelingsovereenkomst (WGBO).

Als gegevens worden beschermd door het beroepsgeheim en anderen dan de hulpverlener hiermee aan de slag willen, bijvoorbeeld onderzoekers, dan moeten zij eerst nagaan of de WGBO gegevensverstrekking uit het medisch dossier toestaat. Is dat het geval, dan dient aan de (U)AVG-voorwaarden te zijn voldaan. Het is voor de praktijk van belang scherp te hebben hoe de WGBO- en (U)AVG-regels zich tot elkaar

verhouden. Bijvoorbeeld om te voorkomen dat er ongeoorloofde verstrekkingen plaatsvinden uit het dossier of dat een verstrekking wordt geweigerd, terwijl dit wel had gemogen.

Er bestaat onduidelijkheid over een juiste toepassing van de (U)AVG- en WGBO-regels. In onze reactie noemen wij drie onduidelijkheden die de wetgever kan wegnemen (paragraaf 1.3.1). Daarnaast vragen wij aandacht voor de gegevensverwerkingen die een hulpverlener volgens de UAVG met gezondheidsgegevens mag verrichten. Hoe dienen deze verwerkingen voor 'een goede behandeling of verzorging c.q. beheer van beroepspraktijk' worden opgevat, bijvoorbeeld in het licht van moderne toepassingen als AI? (paragraaf 1.3.2).

1.3.1 Verduidelijking gewenst over verhouding UAVG en WGBO-begrippen

Het is niet altijd eenvoudig vast te stellen hoe de WGBO toegepast moet worden naast de AVG. Diverse bepalingen uit beide wetten lijken op elkaar, maar hebben elk hun eigen ontstaansgeschiedenis en parlementaire overwegingen gehad. Het is goed dat de wetgever oog heeft voor de verhouding tussen de UAVG en de WGBO, maar enkele onduidelijkheden blijven bestaan.

De (onderzoeks)praktijk is ermee gediend als de wetgever antwoord kan geven op de volgende vragen:

- Is de toestemming van de patiënt voor het verstrekken van gegevens uit het medisch dossier[xxxvii] genoemd in de WGBO materieel hetzelfde als uitdrukkelijke toestemming genoemd in de UAVG?[xxxviii]

Het is aannemelijk dat de toestemmingen voor gegevensverwerkingen uit beide wetten hetzelfde zijn, maar in de literatuur wordt dat tegengesproken.[xxxix] Het antwoord hierop is relevant, omdat het Comité van EU-privacytoezichthouders (EDPB) een 'breed geformuleerde toestemming' voor medisch data-onderzoek moeilijk verenigbaar acht met de AVG[xl], terwijl in de literatuur wordt betoogd dat een dergelijke toestemming wel mogelijk is omdat de WGBO dit toestaat.[xli]

- Vereisen zowel de WGBO als de UAVG dat resultaten van verwerkingen voor wetenschappelijk onderzoek of statistische doeleinden – die de volksgezondheid kunnen dienen – publiekelijk beschikbaar moeten zijn?

Dit is eveneens voor de onderzoekspraktijk van belang, omdat het praktisch is als beide wetten inhoudelijk gelijk zijn met betrekking tot de eis dat het onderzoek wel (of niet) moet leiden tot publieke resultaten. Volgens ex-minister Bruins moeten resultaten van onderzoek in de regel gepubliceerd worden.[xlii] Hij deed deze uitspraak in de context van de UAVG. Dit terwijl de AVG publicatie niet expliciet verplicht en dit soms ook niet mogelijk is. Welke opvatting is juist?

- Is de voorwaarde dat 'het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost'[xliii] materieel gelijk aan de WGBO[xliv] en de AVG-bepalingen inzake kennisgeving aan betrokkenen?[xlv]

Het is nodig zeker te weten of de criteria uit de UAVG en WGBO gelijk zijn, omdat de EDPB van mening is dat er geen gradaties van onmogelijkheid bestaan,[xlvi] terwijl de WGBO-criteria op dit punt veel genuanceerder zijn. Voor de praktijk zou het handig zijn als beide criteria materieel gelijk aan elkaar zouden zijn. Anders kunnen er situaties ontstaan waarin er onder de WGBO geen en onder de UAVG wel toestemming gevraagd moet worden voor medisch data-onderzoek.

1.3.2 Reikwijdte ‘goede behandeling of verzorging c.q. beheer van beroepspraktijk’

Tot slot vragen wij de wetgever aandacht voor het volgende. Uit artikel 30 lid 3 sub a UAVG volgt dat hulpverleners gezondheidsgegevens mogen verwerken voor zover dit noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk. Inhoudelijk is deze bepaling onveranderd ten opzichte van de Wbp.[xlvii] De Wbp sloot destijds aan bij de diverse functies van gegevensverwerking die meestal binnen de gezondheidszorg worden onderscheiden (afgezien van wetenschappelijk onderzoek). De Wbp-wetgever lichtte toe dat het waarborgen van de kwaliteit van de verleende zorg onder ‘beheer’ valt. De EU-privacytoezichthouders hebben daarbij aangeven dat beheer ook facturering, boekhouding of statistiek omvat.[xlviii]

De vraag die rijst is hoe de uitzondering op het verbod om medische gegevens te verwerken anno 2020 geïnterpreteerd moet worden. Met andere woorden: wat is de reikwijdte voor hulpverleners om gezondheidsgegevens te mogen verwerken, wanneer is die grens bereikt en is toestemming van de patiënt vereist voor de gegevensverwerking? Mogen alle situaties die in de zorgpraktijk worden gestoeld op ‘veronderstelde toestemming’ worden geschaard onder dit artikel van de UAVG? Denk aan gegevensverstrekkingen vanwege doorverwijzingen of bepaalde kwaliteitsdoeleinden.

Ook rijst de vraag in hoeverre een hulpverlener moderne toepassingen met AI, zoals *machine learning* of *natural language processing*, mag (laten) uitvoeren ten aanzien gezondheidsgegevens in het medisch dossier. Bijvoorbeeld ten behoeve van een product dat door de dossiergegevens te analyseren de hulpverlener kan assisteren met het opstellen van diagnoses. Past dergelijke productontwikkeling binnen artikel 30 lid 3 sub a UAVG of dient het verbod op de verwerking van gezondheidsgegevens op andere wijze te worden opgeheven, bijvoorbeeld door uitdrukkelijke toestemming van de patiënt? De wetgever zou kunnen verduidelijken hoe het wetsartikel geïnterpreteerd dient te worden in het licht van technologische ontwikkelingen als AI.

2 Hoe verder?

Vorig jaar gaf het kabinet aan het wenselijk te vinden om bij nieuwe technologische ontwikkelingen systematisch na te denken over de risico’s die deze technieken voor de privacy hebben.[xlix]

Het is goed dat het kabinet kwesties als privacy zal agenderen, maar de tijd is inmiddels rijp voor reguleren. De technische ontwikkelingen en maatschappelijke opvattingen dwingen hiertoe. De UAVG biedt kansen om de verwerking van genetische gegevens en biometrische gegevens te reguleren. Met betrekking tot de omgang met gezondheidsgegevens kan het nodige worden verduidelijkt in de UAVG. De wetgever is nu aan zet.

Samenvattend stellen wij als oplossingsrichtingen voor:

1. Verbied de verwerking van genetische gegevens door commerciële analysebureaus en door werkgevers of, als er niet tot een verbod wordt overgegaan, scherp de regels aan voor de omgang met genetische gegevens;
2. Verbied de verwerking van biometrische gegevens in de publieke ruimte en voer voor overige gevallen een vergunningsplicht in;
3. Maak duidelijk wat de voorwaarden zijn voor de verwerking van gezondheidsgegevens in het medische domein (WGBO) en daarbuiten (UAVG) en geef aan welke persoonsgegevens door een hulpverlener verwerkt mogen worden in het kader van een ‘goede behandeling of verzorging c.q. beheer van de beroepspraktijk’.

3 Lees meer

- Werken op waarde geschat (2020)
- Tekort aan democratische controle over digitalisering (2019)
- Forensisch onderzoek – BAP (2019)
- Bescherm de rechten van de mens achter DNA-data (2019)
- Gezondheid Centraal en BAP (2019)
- Doelgericht digitaliseren (2018)
- Wat is de mens? (2018)
- Human Rights in the Robot Age (2017)
- Opwaarderen (2017)
- Dicht op de huid (2015)
- Making perfect life: European governance challenges in 21st century bio-engineering (2012)

4 Eindnoten

[i] Voor zover deze gegevens de genetische kenmerken van een persoon betreffen, vallen ze onder de noemer “genetische gegevens”. Artikel 28 UAVG is dan van toepassing, al dan niet tegelijkertijd met andere regelingen zoals die over etnische gegevens of gezondheidsgegevens.

[ii] Sero D, Zaidi A, Li J, et al. Facial recognition from DNA using face-to-DNA classifiers. *Nat Commun*. 2019;10(1):2557. Published 2019 Jun 11. doi:10.1038/s41467-019-10617-y.

[iii] PCMag, 'This Wearable Helps You Pick Groceries Based on Your DNA', 29 januari 2020, https://www.pcmag.com/news/this-wearable-helps-you-pick-groceries-based-on-your-dna.

[iv] Kool, L., J. Timmer, L. Royakkers en R. van Est, *Opwaarderen - Borgen van publieke waarden in de digitale samenleving*. Den Haag, Rathenau Instituut 2017, p. 36.

[v] Erlich Y, Shor T, Pe'er I, Carmi S. Identity inference of genomic data using long-range familial searches. *Science*. 2018;362(6415):690-694. doi:10.1126/science.aau4832.

[vi] Emily Christofides & Kieran O’Doherty (2016) Company disclosure and consumer perceptions of the privacy implications of direct-to-consumer genetic testing, *New Genetics and Society*, 35:2, 101-123, DOI: 10.1080/14636778.2016.1162092.

[vii] https://nos.nl/op3/artikel/2281182-aanbieders-commerciele-dna-tests-voldoen-vaak-niet-aan-privacywetgeving.html en https://www.consumentenbond.nl/nieuws/2020/commerciele-dna-tests-overdreven-claims-en-slechte-privacy.

[viii] Kalokairinou, L., Howard, H. C., Slokenberga, S., Fisher, E., Flatscher-Thöni, M., Hartlev, M., van Hellemondt, R., Juškevičius, J., Kapelenska-Pregowska, J., Kováč, P., Lovrečić, L., Nys, H., de Paor, A., Phillips, A., Prudil, L., Rial-Sebbag, E., Romeo Casabona, C. M., Sándor, J., Schuster, A., Soini, S., … Borry, P. (2018). Legislation of direct-to-consumer genetic testing in Europe: a fragmented regulatory landscape. *Journal of community genetics*, *9*(2), 117–132. https://doi.org/10.1007/s12687-017-0344-2.

[ix] In deze context is de “uitdrukkelijke toestemming” van de betrokkene de enige juridisch houdbare route, zoals de minister dat eerder aangaf in beantwoording van Kamervragen over bedrijven die DNA-materiaal van hun cliënten met anderen delen: https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2018D51565&did=2018D51565.

[x] Artikel 29 Werkgroep, 'Werkdocument over genetische gegevens', WP91, Goedgekeurd op 17 maart 2004, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf.

[xi] L. Van Lonkhuyzen, ‘Laat DNA-test zien of je sociaal bent op je werk?’, NRC Handelsblad, 11 januari 2018. https://www.nrc.nl/nieuws/2018/01/11/laat-dna-test-zien-of-je-sociaal-bent-op-je-werk- a158784.

[xii] Zoals artikel 5 van de Wet Medische Keuringen.

[xiii] In de overweging verduidelijkt de AVG daarnaast dat zodra een foto wordt verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken, een foto-element dan valt onder de definitie van biometrische gegevens (overweging 51 AVG).

[xiv] https://venturebeat.com/2020/01/04/typingdna-raises-7-million-for-ai-that-identifies-people-by-how-they-type/.

[xv] Kool, L., E. Dujso, en R. van Est (2018). *Doelgericht digitaliseren -Hoe Nederland werkt aan een digitale transitie waarin mensen en waarden centraal staan*. Den Haag: Rathenau Instituut, p. 50, https://www.rathenau.nl/sites/default/files/2018-09/Doelgericht%20digitaliseren.pdf.

[xvi] https://www.farfaces.net/.

[xvii] Digital Trends, ' U.S. military facial recognition could identify people from 1 km away ', 18 februari 2020, https://www.digitaltrends.com/cool-tech/military-facial-recognition-tech-kilometer/.

[xviii] Trouw, ‘Pas op voor de paspop, want hij/zij kijkt ook naar jou’, 23 november 2012, https://www.trouw.nl/nieuws/pas-op-voor-de-paspop-want-hij-zij-kijkt-ook-naar-jou~be33fffc/.

[xix] Zie over een Poolse gezichtsherkenningstool genaamd “PimEyes”: BBC, 'PimEyes facial recognition website 'could be used by stalkers'', 11 juni 2020, https://www.bbc.com/news/technology-53007510.

[xx] Gebruik voor “law enforcement” is waaschijnlijk niet toegestaan, aldus de EDPB: “*The EDPB has doubts as to whether any Union or Member State law provides a legal basis for using a service such as offered by Clearview AI. Therefore, as it stands and without prejudice to any future or pending investigation, the lawfulness of such use by EU law enforcement authorities cannot be ascertained*.”, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf.

[xxi] In de literatuur geconstateerde privacyrisico's zijn, althans in horizontale relaties: ondoorzichtige informatieverzameling, autonomie onder druk, bias en fouten in gezichtsherkenning, einde van anonimiteit, afhankelijkheid van anderen, secundair gebruik van data, machtsongelijkheid en chilling effect. Zie: Keymolen, E., Noorman, M., Sloot, B. van der, Cuijpers, C., Koops, B.-J., Zhao, B., *Op het eerste gezicht - Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties*, Tilburg: Universiteit van Tilburg - Tilburg Institute for Law, Technology, and Society (TILT) 2020, https://www.wodc.nl/onderzoeksdatabase/2992-beperking-privacyrisicoes-toepassing-gezichtsherkenningstechnologie.aspx.

[xxii] Van Est, R. & J.B.A. Gerritsen, with the assistance of L. Kool, *Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality – Expert report written for the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe (PACE)*, The Hague: Rathenau Instituut 2017, https://www.rathenau.nl/sites/default/files/2018-02/Human%20Rights%20in%20the%20Robot%20Age-Rathenau%20Instituut-2017.pdf.

[xxiii] Minister van Binnenlandse Zaken en Koninkrijksrelaties m.b.t. Kabinetsreactie op de rapporten 'Opwaarderen. Het borgen van publieke waarden' en 'Mensenrechten in het robottijdperk' d.d. 9 maart 2018, https://www.rijksoverheid.nl/documenten/brieven/2018/03/09/kabinetsreactie-op-rapporten-opwaarderen.-het-borgen-van-publieke-waarden-en-mensenrechten-in-het-robottijdperk.

[xxiv] Europese Commissie, 'WHITE PAPER - On Artificial Intelligence -A European approach to excellence and trust', 19 februari 2020, COM(2020) 65 final, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[xxv] Raad van Europa: "*Use of Biometric identification systems in publicly accessible spaces, by way of exception to the current general prohibition, should not take place until a specific guideline or legislation at EU level is in place.*" https://rm.coe.int/coe-contribution-to-ec-white-paper-final/16809ee0dd#page=1&zoom=auto,-274,842.

[xxvi] EDPS: "*Support the idea of a moratorium on the deployment, in the EU, of automated recognition in public spaces of human features, not only of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, so that an informed and democratic debate can take place*." https://edps.europa.eu/sites/edp/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf. Zie verder: https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-european-commissions-white-paper_en.

[xxvii] EUObserver, 'Facial-recognition moratorium back on EU agenda', 3 juli 2020, https://euobserver.com/science/148839.

[xxviii] "*The GDPR adds an additional requirement when it comes to legitimizing the processing of special categories of data(sensitive data). The processing should not only be in the public interest, but in the 'substantial' public interest. The GDPR does not specify what is to be regarded as substantial.*" (ond. Rathenau Instituut), in: Hoofnagle, Chris Jay and van der Sloot, Bart and Zuiderveen Borgesius, Frederik, The European Union General Data Protection Regulation: What It Is And What It Means (September 24, 2018). *UC Berkeley Public Law Research Paper*. Available at SSRN: https://ssrn.com/abstract=3254511 or http://dx.doi.org/10.2139/ssrn.3254511.

[xxix] Fundamental Rights Agency (FRA), 'Your rights matter: Data protection and privacy - Fundamental Rights Survey', 18 juni 2020, https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection

[xxx] N. Waarlo en L. Verhagen, 'De stand van gezichtsherkenning in Nederland', *de Volkskrant*, 27 maart 2020, https://www.volkskrant.nl/kijkverder/v/2020/de-stand-van-gezichtsherkenning-in-nederland~v91028/.

[xxxi] Artikel 33 lid 4 sub c en lid 5 UAVG. Met betrekking tot biometrische toepassingen hanteert Denemarken reeds een vergunningsplicht, zie: European Digital Rights (EDRi), 'Danish DPA approves Automated Facial Recognition', 19 juni 2019, https://edri.org/danish-dpa-approves-automated-facial-recognition/.

[xxxii] Voor voorbeelden met betrekking tot migranten, zie: FRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, maart 2018.

[xxxiii] Ter illustratie, de Autoriteit Persoonsgegevens in haar beslissing van 4 december 2019 over de verwerking van vingerafdrukken van werknemers: *"Ook al zou er wèl sprake zijn van toestemming, dan zou deze ook nog eens 'vrijelijk gegeven' moeten zijn. Dit betekent dat er geen dwang achter mag zitten of dat toestemming een voorwaarde is voor iets anders. Werknemers hebben echter aangegeven dat het scannen van de vingerafdruk verplicht was. (...) Gezien de afhankelijkheid die het gevolg is van de relatie tussen werkgever en werknemer, is het onwaarschijnlijk dat de werknemer zijn of haar toestemming vrijelijk kon verlenen.",* https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_vingerafdrukken_personeel.pdf.

[xxxiv] Privacytoezichthouders in Zweden en Polen vonden reeds biometrische toepassingen ontoelaatbaar op scholen. Zweden: https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en. Polen: https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en.

[xxxv] Hof van Justitie EU 6 november 2003, CLI:EU:C:2003:596 (*Lindqvist*).

[xxxvi] Artikel 4 lid 15 AVG.

[xxxvii] Artikel 7:457 lid 1 BW.

[xxxviii] Artikel 22 lid 2 sub a UAVG en artikel 24 sub c UAVG.

[xxxix] Ploem et al., 'Medisch data-onderzoek in het AVG-tijdperk: een zoektocht naar de juiste regels', *Tijdschrift voor Gezondheidsrecht* 2020/2.

[xl] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.0, Adopted on 4 May 2020, 154 e.v., https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[xli] Artikel 24 sub b UAVG, 7:458 lid 2 sub a BW.

[xlii] Kamerbrief van de Minister voor Medische Zorgen en Sport m.b.t. reactie op artikel over secundair gebruik data d.d. 4 oktober 2019, https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/04/kamerbrief-over-reactie-artikel-fd-over-secundair-gebruik-data.

[xliii] Artikelen 24 sub c en 28 lid 3 UAVG.

[xliv] Artikel 7:458 lid 1 sub a en b Burgerlijk Wetboek.

[xlv] Artikel 14 lid 5 sub b en 19 AVG.

[xlvi] EDPB Richtsnoeren 3/2020 inzake de verwerking van gezondheidsgegevens voor wetenschappelijk onderzoek in het kader van de COVID-19-uitbraak, Vastgesteld op 21 april 2020, punt 36. De EDPB doet deze uitspraak in de context van artikel 14 lid sub b AVG.

[xlvii] De Wbp-bepaling wilde hiermee aansluiten bij de Privacyrichtlijn 95/46/EG, de voorganger van de AVG. Meer precies: artikel 8 lid 3 Privacyrichtlijn 95/46/EG. Deze betreft "*de verwerking van de gegevens [die] noodzakelijk is voor de doeleinden van preventieve geneeskunde of medische diagnose, het verstrekken van zorg of behandelingen of het beheer van gezondheidsdiensten en wanneer die gegevens worden verwerkt door een gezondheidswerker die onderworpen is aan het in de nationale wetgeving, of in de door nationale bevoegde instanties vastgestelde regelgeving, vastgelegde beroepsgeheim of door een andere persoon voor wie een gelijkwaardige geheimhoudingsplicht geldt.*" Vgl. artikel 9 lid 2 sub h AVG: "*de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen*."

[xlviii] Article 29 Working Party, 'WP 131 - Working Document on the processing of personal data relating to health in electronic health records (EHR)', Adopted on 15 February 2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf.

[xlix] Brief van de Minister voor Rechtsbescherming m.b.t. Initiatiefnota van het lid Koopmans: Onderlinge privacy d.d. 7 juni 2019, https://zoek.officielebekendmakingen.nl/kst-34926-8.html.