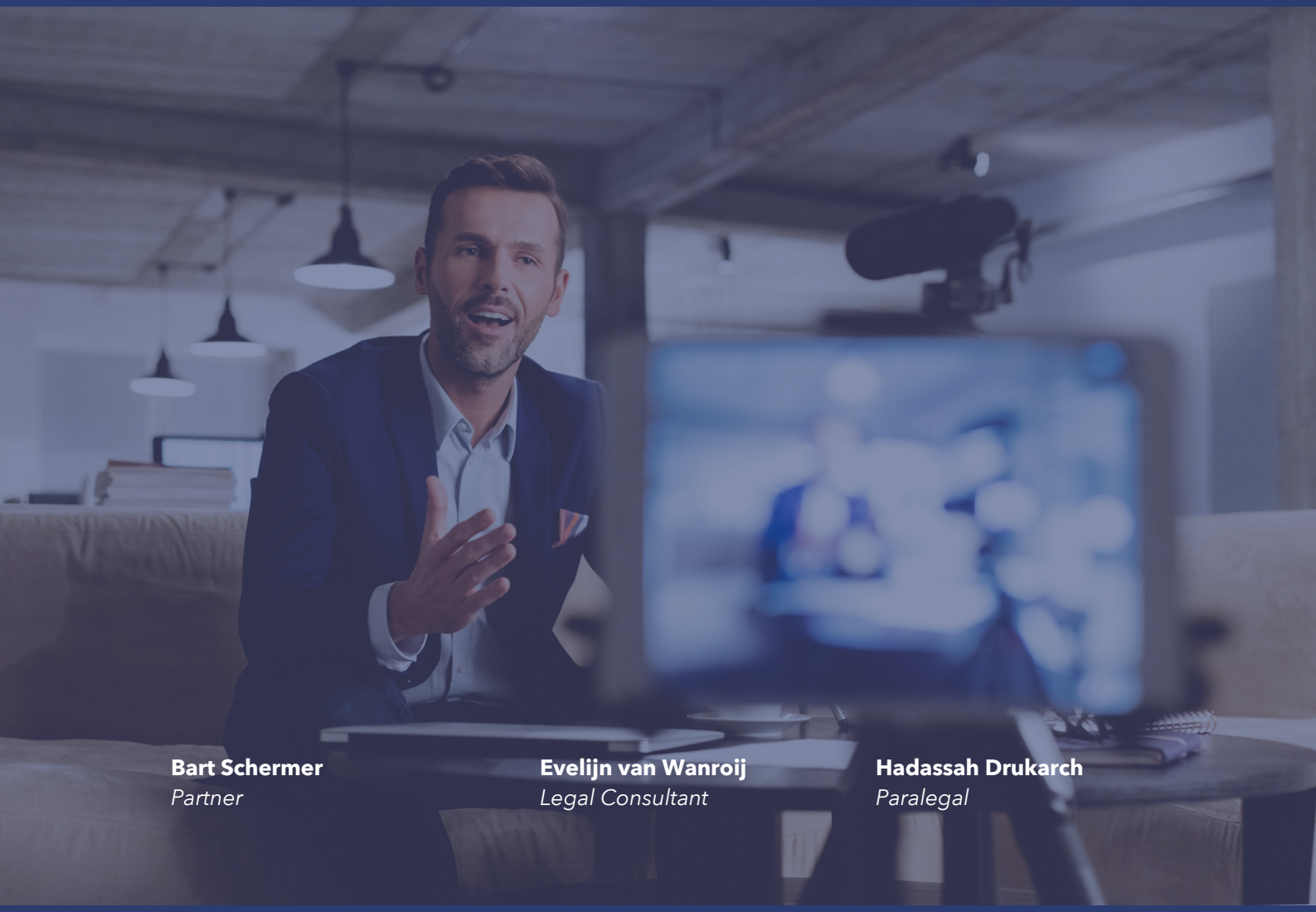
CONSIDERATI

LEGAL | PUBLIC AFFAIRS | RESPONSIBLE TECH

Generieke verkenning van juridische randvoorwaarden voor de toepassing van spraakherkenning en autotranscriptie in het JenV-domein

Considerati
23 december 2022



Bart Schermer
Partner

Evelijn van Wanroij
Legal Consultant

Hadassah Drukarch
Paralegal

Management samenvatting

Sinds begin 2020 wordt binnen het JenV-beleidsteam Artificial Intelligence onderzoek gedaan naar de mogelijke toepassingen van AI binnen het JenV-domein. Ook is er door verschillende organisaties in het JenV-domein in de afgelopen jaren ervaring opgedaan met AI-toepassingen.

Meer recentelijk is binnen het JenV-domein interesse ontstaan voor de toepassing van spraakherkenning en autotranscriptie. Door het geautomatiseerd vastleggen van gesprekken, verhoren, vergaderingen wordt met name een hoop tijd bespaard. De bespaarde tijd kan worden ingezet om de primaire taken beter uit te voeren, de dienstverlening aan de burger te verbeteren en de waarheidsvinding te versterken.

De toepassing van spraakherkenning binnen het JenV-domein roept de vraag op onder welke voorwaarden dit op een legitieme manier kan worden toegepast. Dit rapport brengt aan de hand van verschillende *use cases* binnen het JenV-domein de juridische kaders en voorwaarden in kaart waaronder spraakherkenning en autotranscriptie verantwoord kunnen worden toegepast binnen het werkveld van JenV.

Spraakherkenning is een uitwerking van spraaktechnologie en richt zich op het automatisch en met behulp van AI omzetten van natuurlijke spraak(signalen) in een transcript daarvan. Daarmee kan spraakherkenning onderscheiden worden van andere uitwerkingen van spraaktechnologie, waaronder stemherkenning, sprekerherkenning en spraaksynthese. Voordat spraakherkenningssystemen bruikbaar zijn, worden zij met behulp trainingsdata getraind. Vervolgens vertrouwt de technologie grotendeels op de kracht van computers om een relevant spraaksignaal op te vangen, patronen in het opgevangen spraaksignaal te herkennen en dit spraaksignaal vervolgens om te zetten in de tekstuele weergave daarvan. De technische werking van spraakherkenning is nader uiteengezet in hoofdstuk 2.

Spraakherkenning en autotranscriptie kunnen bij verschillende organisaties binnen het JenV-domein worden ingezet. In dit rapport bespreken we de inzet van deze technologie bij de Nationale Politie, de Reclassering en een fictieve organisatie binnen het justitiedomein. Er is gekozen voor deze drie *use cases* omdat ze ieder binnen een ander privacyrechtelijk kader vallen (AVG, Wpg en de Wjsg). Dit stelt ons in staat om juridische vraagstukken vanuit deze verschillende wettelijke kaders te beschouwen. In hoofdstuk 3 wordt nader ingegaan op de toepassing van spraakherkenning en autotranscriptie binnen deze organisaties.

Dit rapport brengt vervolgens de juridische kaders in kaart die van toepassing zijn bij het ontwikkelen en inzetten van spraakherkenning en autotranscriptie binnen het JenV-domein. Hierbij staan we stil bij het juridische kader ten aanzien van privacy en gegevensbescherming (de AVG, de Wpg en de Wjsg). Welke van deze regimes van toepassing is, hangt af van de JenV-organisatie, de persoonsgegevens die worden verwerkt en het doel van de verwerking. Het gevolg hiervan is dat er verschillende regimes van toepassing kunnen zijn op een reeks verwerkingen die achter of naast elkaar plaatsvinden. Daarnaast staan we in dit rapport stil bij overige juridische kaders die van toepassing zijn op de ontwikkeling en inzet van spraakherkenning en autotranscriptie binnen het JenV-domein: de Europese AI-verordening, Modernisering Wetboek van Strafvordering, de Algemene Wet Bestuursrecht en de Archiefwet.

Op basis van deze juridische kaders, onderzoeken we onder welke juridische voorwaarden spraakherkenning verantwoord toegepast kan worden binnen het JenV-domein. We beantwoorden deze vraag aan de hand van een aantal deelvragen die met name toezien op de vereisten en beperkingen die juridische kaders stellen aan:

- het verkrijgen van toestemming voor het gebruik van autotranscriptie;
- het opslaan van integrale audio-opnames van gesprekken en transcripties daarvan;
- het trainen van spraakherkenning met trainingsdata; en
- het afnemen van spraaktechnologie uit de markt en samenwerking met derden.

Met betrekking tot de eerste deelvraag concluderen wij dat toestemming in de meeste gevallen binnen het JenV-domein geen geschikte grondslag is voor het trainen en gebruiken van spraakherkenningsmodellen, omdat de toestemming niet kan voldoen aan de vereisten die de AVG hieraan stelt (vrijelijk gegeven, specifiek, geïnformeerd en ondubbelzinnig). Met name het vereiste dat toestemming vrijelijk moet worden gegeven is moeilijk binnen de JenV context te realiseren. In gevallen waarin een ongelijke verhouding bestaat tussen de betrokkene en de verwerkingsverantwoordelijke, wordt toestemming niet als vrij aangemerkt. De verhouding tussen JenV en de betrokkene (dader, slachtoffer, werknemer) kan als ongelijk worden bestempeld waardoor toestemming niet aan alle vereisten uit de AVG voldoet. In plaats van toestemming kan de verwerking van persoonsgegevens worden gerechtvaardigd door andere grondslagen uit de AVG. De grondslagen noodzakelijk voor de uitvoering van een taak van algemeen belang of openbaar gezag (6e AVG) en het gerechtvaardigd belang van de verwerkingsverantwoordelijke (6f AVG) liggen daarbij voor de hand. Vanuit de Wpg en de Wjsg kan de taakstelling van de betreffende organisatie als grondslag dienen. In hoofdstuk 8 van dit rapport gaan we nader in op deze grondslagen.

In dit rapport wordt ook onderzocht hoe lang audio-opnamen van gesprekken en transcripties daarvan bewaard mogen worden. Het antwoord op deze vraag hangt af van juridisch kader dat van toepassing is. Het uitgangspunt van de AVG is dat persoonsgegevens niet langer waard mogen worden als dat noodzakelijk is voor de doeleinden van de verwerking. Organisaties waarop de AVG van toepassing is, zoals de Reclassering bepalen zelf hoe lang het nodig is om persoonsgegevens (zoals de audio-opnames) te bewaren om de voorgenomen doeleinden te bereiken. Voor de politie geldt dat persoonsgegevens – waaronder audio-opnamen en transcripties daarvan – verwijderd of vernietigd moeten worden wanneer deze niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verwerkt of dit door een wettelijke bepaling wordt vereist. Aan de hand van de in de Wpg genoemde bewaartermijnen moet de politie beoordelen hoe lang zij de gegevens mag bewaren. De Wjsg stelt dat de Minister van Veiligheid en Justitie de nodige maatregelen treft om te verzekeren dat justitiële gegevens worden verwijderd of vernietigd

zodra deze niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verwerkt of waar dit door enige wettelijke bepaling wordt vereist. Zo is het mogelijk dat voor bepaalde categorieën Wjsg-gegevens specifieke bewaartermijnen gelden die in de Wjsg worden gespecificeerd. Met betrekking tot de bewaartermijn van de gegevens verdient het opmerking dat de genoemde regels niet afwijken waar het gaat om metadata.

Uit dit onderzoek blijkt dat persoonsgegevens, politiegegevens of Wjsg-gegevens mogen worden (her)gebruikt voor het trainen van een spaakherkenningssysteem wanneer een van de volgende punten van toepassing is:

- het trainen past binnen de doelomschrijving van het primaire proces waarin de audio opnamen zijn gemaakt;
- de nieuwe verwerking (training) verenigbaar is met de oorspronkelijke verwerking;
- er is sprake van een wettelijke regeling die training mogelijk maakt (bijvoorbeeld in de Wpg, de Wjsg of andere wetgeving).

Met betrekking tot het laatste punt moet worden opgemerkt dat er op het moment van schrijven van dit rapport nog geen wettelijke regeling is waarin dit is opgenomen.

Met betrekking tot de derde deelvraag blijkt uit dit onderzoek dat er vanuit het perspectief van gegevensbescherming geen specifieke bezwaren bestaan tegen het gebruiken van spraakherkenningsmodellen van commerciële partijen. Bij het gebruik van spraakherkenningsmodellen van derden is het wel van groot belang hoe het gebruik van het model technisch en organisatorisch is ingericht. Daarbij geldt dat de partij die het spraakherkenningsmodel aanbiedt een verwerker is voor JenV. Voor het versturen van persoonsgegevens naar deze partijen (trainingsdata en/of input data) gelden de regels van de AVG (danwel Wpg of Wjsg). In het bijzonder van belang zijn de contractuele afspraken met verwerkers, de beveiliging en gegevensdoorgifte buiten Europa. Daarnaast moet aangesloten worden bij de Rijksbrede strategie voor het gebruik van clouddiensten en de beveiligingsvereisten zoals vastgelegd in onder andere de BIO. Hierin is onder meer

bepaald dat het niet is toegestaan om clouddiensten te gebruiken voor staatsgeheim gerubriceerde informatie.

In dit rapport is ook onderzocht welke risico's voor de (privacy van) betrokkene ontstaan door spraakherkenning en autotranscriptie en welke maatregelen genomen kunnen worden om deze risico's te mitigeren. We bespreken hieronder de hoofdpunten van deze analyse en verwijzen voor een verdere uitwerking naar hoofdstuk 7 van dit rapport.

Een eerste risico van de inzet van spraakherkenning en autotranscriptie in het justitiedomein is gelegen in het feit dat de technologie die hieraan ten grondslag ligt niet feilloos is. Hoewel niet uniek aan spraakherkenning, kunnen fouten en incompleetheden in transcripten tot verkeerde conclusies en/of beslissingen leiden. Het is niet de verwachting dat deze technologie in de toekomst feilloos zal worden. Om dit risico te mitigeren, adviseren wij daarom vanuit een organisatorisch perspectief om maatregelen ter controle van fouten in transcripties - een (handmatige) dubbelcheck - te treffen en aanvullende (menselijke) controles in te bouwen. Vanuit een technisch oogpunt adviseren wij het proces van controle te vergemakkelijken door transcripties en audiobestanden aan elkaar te koppelen.

Een ander risico van de inzet van spraakherkenning en autotranscriptie binnen het justitiedomein ligt in de mogelijke uitsluiting van bepaalde groepen vanwege een gebrek aan voldoende representativiteit in de gebruikte spraaktechnologie. De aard en de ernst van dit risico is afhankelijk van de organisatorische inbedding. Om dit risico te mitigeren raden wij aan om bij het trainen van spraakherkenningsmodellen binnen het JenV-domein gebruik te maken van trainingsdata die een zo groot mogelijke inhoudelijke diversiteit en inclusiviteit garanderen en van voldoende kwaliteit zijn. Ook is het van belang om inputdata van een zo hoog mogelijke kwaliteit te gebruiken bij de inzet van spraakherkenning. Daarnaast adviseren wij met het oog op de mogelijke uitsluiting van bepaalde groepen personen om alternatieven te bieden waar spraakherkenning tekortschiet en aanvullend menselijk toezicht in te bouwen en deze maatregelen goed te documenteren. Vanuit een

technisch oogpunt raden wij tot slot aan gevoelige categorieën persoonsgegevens, die op basis van privacywetgeving niet worden beschouwd als bijzondere categorieën persoonsgegevens, te behandelen alsof ze hier wel toe behoren. Bijzondere categorieën persoonsgegevens genieten een hogere bescherming onder de privacywetgeving omdat verwerking hiervan een groter risico met zich meebrengt.

Tot slot vormt het delen van persoonsgegevens met partijen buiten de justitieketen een risico. Wanneer gebruik wordt gemaakt van spraakherkenningsmodellen van commerciële partijen, dan is de kans groot dat (gevoelige) gegevens gedeeld moeten worden met deze partijen. De aard en de ernst van dit risico is afhankelijk van de gevoeligheid van de gegevens en de context waarin de spraakherkenning wordt toegepast. Om dit risico te mitigeren wordt geadviseerd om vanuit een organisatorisch perspectief in de vorm van een verwerkersovereenkomst duidelijke afspraken te maken met verwerkers buiten de justitieketen om te voorkomen dat zij onbegrensd toegang hebben tot persoonsgegevens. Verder is het van belang ten aanzien van informatie die wegens de gevoeligheid daarvan niet met derden gedeeld kan worden, het leidende beleid daaromtrent (bijvoorbeeld het Rijksbrede cloudbeleid) in acht te nemen. Vanuit een technisch oogpunt moet gedacht worden aan maatregelen als anonimisering, pseudonimisering, toegangscontrole en encryptie. Deze maatregelen maken reeds onderdeel uit van de informatiebeveiligingsvereisten voor de overheid. Het is raadzaam te bekijken in hoeverre deze maatregelen al toegepast / toepasbaar zijn in de context van spraakherkenning.

Inhoudsopgave

Lijst van afkortingen

ABBB	Algemene beginselen van behoorlijk bestuur
AI	Artificiële Intelligentie
AP	Autoriteit Persoonsgegevens
ASR	Automatic Speech Recognition
AVG	Algemene verordening gegevensbescherming
AVR	Audiovisuele registratie verhoor
AVT	Audio verhoor transcriptie
Awb	Algemene wet bestuursrecht
Bjsg	Besluit justitiële en strafvorderlijke gegevens
Bpg	Besluit politiegegevens
DG SenB	Directoraat-Generaal Straffen en Beschermen
DL	Deep Learning
EC	Europese Commissie
EVRM	Europees Verdrag voor de Rechten van de Mens
GGP	Gebiedgebonden politie
HMM	Hidden Markov Models
JenV	Justitie en Veiligheid
ML	Machine Learning
NLP	Natural Language Processing
OM	Openbaar Ministerie
PR	Pattern Recognition
SD	Speaker Diarization
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
Wob	Wet openbaarheid van bestuur
Woo	Wet open overheid
Wpg	Wet politiegegevens
Wjsg	Wet justitie en strafrechtelijke gegevens

1 Inleiding

Het Ministerie van Justitie en Veiligheid (hierna: 'JenV') zorgt voor de rechtsstaat in Nederland, zodat mensen in vrijheid kunnen samenleven, ongeacht hun levensstijl of opvattingen. Om te zorgen voor een meer veilige en rechtvaardige samenleving, biedt JenV rechtsbescherming en intervenieert zij waar nodig.

Een van de doelen van het beleidsteam AI van JenV is om ervoor te zorgen dat JenV een sterke speler op het gebied van AI is. Om dit doel te bereiken is binnen verschillende organisaties in het JenV-domein in de afgelopen jaren ervaring opgedaan met verschillende AI-toepassingen.

Een veelbelovende toepassing waar binnen het JenV domein veel interesse voor is, is spraakherkenning. In het JenV-domein kan spraakherkenning op diverse manieren bijdragen aan het oplossen van maatschappelijke opgaven en het verbeteren van de dienstverlening aan burgers. Toepassingen die het nut van spraakherkenning binnen het JenV-domein illustreren, zijn onder andere:

- Het geautomatiseerd laten notuleren van gesprekken of verhoren met burgers, rechtszittingen, vergaderingen en andere bijeenkomsten van medewerkers in het justitie- en veiligheidsdomein;
- Het geautomatiseerd verwerken van informatie uit gesproken taal in een informatiesysteem, zoals bij een aangifte, een 112-melding of bij dossieropbouw;
- Het doorzoekbaar maken van audiovisueel materiaal.

1.1 Probleemstelling en onderzoek

De toepassing van spraakherkenning binnen het JenV-domein roept echter wel een aantal vragen op met betrekking tot de legitieme toepassing ervan. De probleemstelling voor dit onderzoek luidt dan ook:

"Onder welke juridische voorwaarden kunnen spraakherkenning en autotranscriptie verantwoord worden toegepast binnen het werkveld van Justitie en Veiligheid?"

Dit rapport brengt aan de hand van verschillende *use cases* binnen het JenV-domein de juridische kaders en voorwaarden in kaart waaronder spraakherkenning verantwoord kan worden toegepast binnen het werkveld van JenV.[1] Om de probleemstelling op te lossen heeft JenV een aantal onderzoeksvragen opgesteld die wij in dit rapport beantwoorden. In de bijlage opgenomen in paragraaf 9.1. staat een volledig overzicht van de onderzoeksvragen.

1.2 Leeswijzer

Dit rapport is als volgt opgebouwd:

Hoofdstuk 2 beschrijft de technische werking en algemene toepassingen van spraakherkenning.

Hoofdstuk 3 gaat in op het toepassingsgebied van spraakherkenning binnen het JenV-domein aan de hand van een aantal *use cases*.

In hoofdstuk 4 behandelen wij het algemene juridisch kader dan van toepassing is op spraakherkenning. Hierbij bespreken wij bestaande wetgeving waarin privacy en omgang met persoonsgegevens worden geregeld zoals de Algemene Verordening

[1] Spraakherkenning is een uitwerking van spraaktechnologie die toeziet op het omzetten van spraak naar tekst (ASR). Spraaktechnologie omvat naast spraakherkenning ook spraaksythese, sprekeronderscheiding, sprekerherkenning, emotiedetectie en spraakassistentie. Binnen de scope van dit onderzoek valt enkel spraakherkenning; de overige vormen van spraaktechnologie vallen buiten de scope van dit onderzoek.

Gegevensbescherming (hierna: 'AVG'), de Wet politiegegevens (hierna: 'Wpg') en de Wet justitiële en strafvorderlijke gegevens (hierna: 'Wjsg').

In hoofdstuk 5 bespreken wij overige wet- en regelgeving die van belang is bij de beantwoording van de deelvragen zoals de draft AI-verordening, mogelijke implicaties van modernisering van het Wetboek van Strafvordering en de Innovatiewet Strafvordering.

In hoofdstuk 6 brengen we vervolgens – op basis van de in hoofdstuk 3 beschreven *use cases* – de juridische kaders en voorwaarden in kaart waaronder spraakherkenning verantwoord kan worden toegepast binnen het werkveld van JenV. In dit hoofdstuk wordt onder meer antwoord gegeven op de onderzoeksvragen die in bijlage 1 van dit rapport zijn opgenomen.

Hoofdstuk 7 biedt een overzicht van de (juridische) risico's die verband houden met de toepassing van spraakherkenning binnen het JenV-domein. Naast het classificeren van de relevante risico's, zal ook een blik worden geworpen op de mogelijke manieren waarop deze kunnen worden gemitigeerd middels beleidsmatige en technische maatregelen.

Hoofdstuk 8 biedt een algemene conclusie, gevolgd door een overzicht met praktische tips ten aanzien van de training, toepassing en inrichting van spraakherkenning binnen JenV in hoofdstuk 9.

Bijlage 1 bij dit rapport biedt een overzicht van de hoofdvraag en deelvragen die door JenV aan Considerati zijn voorgelegd in het kader van dit rapport.

2 Technische werking spraakherkenning

Spraakherkenning of *Automatic Speech Recognition* (ASR) is een patroonherkenningstechnologie die erop gericht is automatisch en met behulp van AI natuurlijke spraak(signalen) om te zetten in een transcript daarvan (zie afbeelding 1). Spraakherkenning werkt door:

- een spraakopname op te splitsen in afzonderlijke geluiden;
- elk geïdentificeerd geluid te analyseren;
- met behulp van algoritmen de waarschijnlijkheid van een bepaald woord in de betreffende taal en in de gegeven context vast te stellen; en
- dat woord in tekst om te zetten.

Afbeelding 1 Simpele weergave van spraakherkenning.

2.1 Spraak

Onder spraak wordt verstaan: *"het vermogen om te praten, de activiteit van het praten of een segment gesproken taal."*[2] Alhoewel spraak de meest directe vorm van talige communicatieve interactie tussen mensen is, ontbreekt een eenduidige definitie. Spraak wordt geproduceerd door nauwkeurig gecoördineerde spierbewegingen in het hoofd, de nek, borst en buik en wordt door mensen gebruikt om gedachten, gevoelens en ideeën mondeling uit te drukken. Spraak wordt geproduceerd door de toevoer van lucht uit de longen naar het strottenhoofd (ademhaling), waar de stembanden open kunnen worden

[2] Cambridge Dictionary. (2022, 30 maart). *speech definition*. Geraadpleegd op 5 april 2022, van https://dictionary.cambridge.org/dictionary/english/speech. Vertaald vanuit het Engels: 'the ability to talk, the activity of talking, or a piece of spoken language'.

gehouden om de lucht door te laten stromen of deze te laten trillen om geluid te produceren (fonatie). Tot slot wordt de luchtstroom uit de longen gevormd door de articulatoren in de mond en neus (articulatie), waarna spraak tot stand komt.[3]

Behalve de daadwerkelijk uitgesproken woorden, bevat spraak een enorme hoeveelheid informatie over en kenmerken van de persoon aan wie de betreffende spraak gekoppeld kan worden. Bewegingen in het menselijke ademhalingssysteem worden continu gereguleerd door het zenuwstelsel. Bepaalde ademhalingscentra in de hersenstam bepalen de ademhalingspatronen op basis van de individuele lichaamsbehoeften op het desbetreffende moment. Het gevolg hiervan is dat onder meer emoties onmiddellijk hoorbaar zijn in de productie van spraak. Voorbeelden hiervan zijn de schuchtere stem van angst, de blaffende stem van woede, de zwakke eentonigheid van melancholie of de rauwe heftigheid tijdens agitatie.[4] Daarnaast biedt spraak ook inzicht in andere kenmerkende eigenschappen van een individu, waaronder geslacht, leeftijd, afkomst (bijvoorbeeld door middel van accent) en gezondheid. Wat dit laatste betreft, geldt bijvoorbeeld dat veel organische ziekten van het zenuwstelsel of van het ademhalingsmechanisme geprojecteerd kunnen worden in de stem van een individu.[5] Bepaalde ziekten van het zenuwstelsel laten de stem bijvoorbeeld trillen; de stem van een astmatisch persoon klinkt moeizaam en kortademig; en bepaalde soorten ziekten die een deel van de hersenen, in het bijzonder het cerebellum, aantasten, veroorzaken een geforceerde en gespannen wijze van ademhaling, zodat de stem extreem laag en grommend klinkt.

Audiosignalen omvatten een brede variatie aan relevante informatie en patronen. Deze kunnen, in tegenstelling tot visuele signalen (bijvoorbeeld foto's en video's), worden onderverdeeld in kleinere subcategorieën.[6] Vooral ten aanzien van spraak geldt dat het geluidssignaal dat zich daarbij voordoet en wordt ontvangen door de luisteraar zijn

[3]

[4] Britannica. (z.d.). *Speech | Language, Voice Production, Anatomy, & Physiology*. Geraadpleegd op 5 april 2022, van https://www.britannica.com/topic/speech-language.

[5] Idem.

[6] Te weten: aan de hand van bepaalde kenmerkende eigenschappen, waaronder periodiciteit, richting, dynamiek, spectrale balans, enzovoorts, kunnen mensen audiosignalen identificeren en deze audiosignalen vormen op hun beurt de basis voor spraakherkenning. Zie ook O'Shaughnessy, D. (2008). Automatic speech recognition: History, methods and challenges. *Pattern Recognition*, *41*(10), 2965-2979. https://doi.org/10.1016/j.patcog.2008.05.008.

oorsprong vindt in het menselijke spraakkanaal. Gezien de specificiteit van de oorsprong van spraaksignalen, is de variabiliteit die zich in het kader hiervan kan voordoen relatief beperkt. Wanneer mensen spraak proberen te herkennen, zullen zij dan ook normaal gesproken elk audiosignaal dat voor hen niet herkenbaar is als afkomstig uit het menselijke spraakkanaal, niet als spraak kwalificeren en die signalen die voor hen wel als spraak herkenbaar zijn, proberen te ontcijferen. Bovendien kunnen spraaksignalen, ondanks de relatief beperkte variabiliteit van patronen, anders worden opgevat afhankelijk van de omgeving en context waarin zij uiting vinden.[7] Elk spraaksignaal is uniek en kan niet op precies dezelfde manier door een mens herhaald worden. Variaties in spraak kunnen zich voordoen en hangen af van: de spreker, externe factoren (bijvoorbeeld achtergrondgeluid) en reducties (zoals: verschil tussen wat is geschreven en wat daadwerkelijk wordt uitgesproken), maar ook accenten, dialecten, volume en toonhoogte kunnen hierbij een rol spelen. Ondanks het feit dat men over het algemeen dezelfde taalkundige regels volgt bij het spreken, variëren spraaksignalen aldus en kunnen afwijkingen in spraak(signalen) zich voordoen.

2.2 Technische werking spraakherkenning

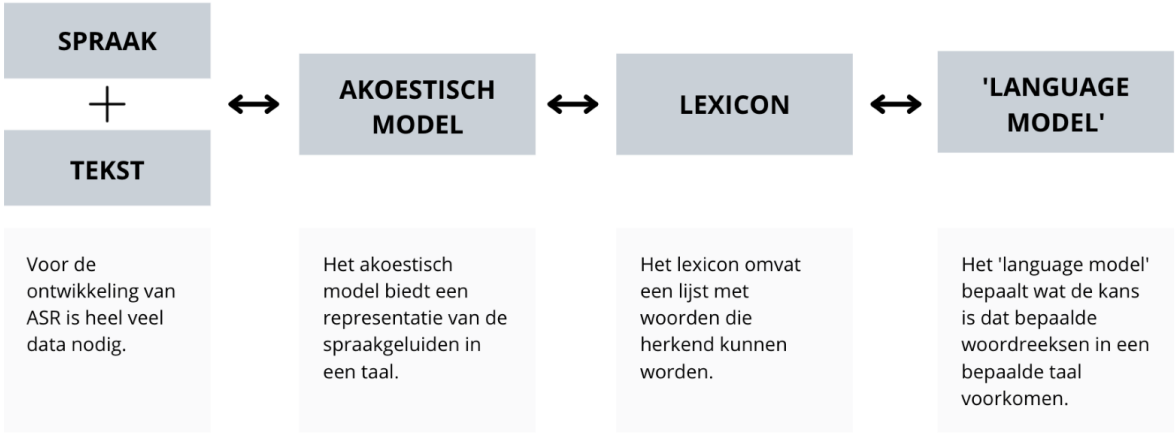
2.2.1 Technische werking

Zoals voor iedere patroonherkenningstechnologie geldt, poogt spraakherkenning patronen in een spraaksignaal te ontdekken. Systemen voor spraakherkenning integreren grammatica, syntaxis, structuur en samenstelling van audio- en spraaksignalen om menselijke spraak in tekst om te zetten die vervolgens kan worden geanalyseerd door een mens of een computer.

Nadat menselijke spraak via een microfoon is gedigitaliseerd, worden algoritmes en modellen ingezet om de relevante woorden te herkennen via een berekening van de waarschijnlijkheid dat het betreffende woord zich op die plaats in het signaal voordoet. Hiertoe wordt gebruik gemaakt van een akoestisch model, een lexicon en een zogeheten 'language model', die elk getraind zijn op basis van historische data (dat wil zeggen voorbeelden van woorden waarmee het systeem getrained is). Het technische model dat

[7] Idem.

wordt gebruikt om spraakherkenning tot stand te brengen, is in afbeelding 2 weergegeven[8]:



Afbeelding 2 Weergave technisch model spraakherkenning (ASR).

Spraakherkenning vertrouwt grotendeels op de kracht van computers om een relevant spraaksignaal op te vangen, patronen in het opgevangen spraaksignaal te herkennen en dit spraaksignaal vervolgens om te zetten in de tekstuele weergave daarvan. Bij spraakherkenning kan een onderscheid worden gemaakt tussen *real time* of *live* spraakherkenning en spraakherkenning achteraf. Real time spraakherkenning houdt in dat spraak live wordt getranscribeerd, waardoor de spraakherkenningstechnologie minder lang de tijd heeft om de spraak te herkennen en om te zetten naar tekst. Spraakherkenning achteraf houdt in dat de spraakherkenningstechnologie een opgenomen audiofragment transcribeert.

Spraakherkenning is een toepassing van het bredere concept spraaktechnologie (zie afbeelding 3) en is de daadwerkelijke omzetting van audio naar tekst. Om spraakherkenning te verbeteren kan sprekeronderscheiding worden toegepast.[9] Hierbij

[8] Uit het interview met de spraaktechnologen kwam naar voren dat binnen het domein van spraakherkenning met name twee open source modellen van belang zijn: het Kaldi model (https://kaldi-asr.org/) en het Wav2vec model (https://huggingface.co/docs/transformers/model_doc/wav2vec2). Een nadere bespreking van deze beide modellen valt buiten de reikwijdte van dit rapport. In dit rapport is het Kaldi model – het tot nog toe meest gebruikte model voor spraakherkenning – als uitgangspunt genomen. Er bestaan ook andere open source modellen (zie bijvoorbeeld https://fosspost.org/open-source-speech-recognition/), maar ook deze laten we in dit rapport buiten beschouwing.
[9] Ook wel sprekerdiarisatie (*speaker diorisation*) genoemd, zie onder.

worden verschillende sprekers onderscheiden in een audiofragment. Verder maakt spraaktechnologie ook het uniek identificeren van een stem mogelijk (een specifieke stem herkennen uit alle andere stemmen), kan het emoties detecteren en kan het gebruikt worden als onderdeel van bijvoorbeeld slimme assistenten.

SPRAAKTECHNOLOGIE: TOEPASSING, VOORBEELDEN EN COMPLEXITEIT	
Spraak assistent (spraakherkenning + automatisch besluitvorming)	Autonome systemen (bijv. Alexa, Siri, etc.)
Emotiedetectie	Vergelijkbaar met leugendetector
Sprekerherkenning	Vergelijkbaar met gezichtsherkenning
Sprekeronderscheiding	Differentiatie (zonder identificatie)
Autotranscriptie (S2T)	Automatische notulering
Spraaksynthese (T2S)	Ondersteuning (bijv. slechtzienden)

COMPLEXITEIT ▲

Afbeelding 3 Spraaktechnologie: toepassingen, voorbeelden en complexiteit.

In dit rapport bepreken wij tenzij anders vermeld de rol van autotranscriptie (S2T) binnen het justitie-domein.

De meest geavanceerde vormen van spraakherkenning die vandaag de dag worden ingezet maken gebruik van *machine learning* (Hierna: 'ML'). ML maakt het mogelijk om waarschijnlijkheden te voorspellen op basis van voorbeelden uit trainingsdata. In de meest recente ontwikkelingen op het gebied van spraakherkenning, spelen hiertoe met name *big data* en *deep learning* (hierna: 'DL') – een tak van ML – een belangrijke rol.[10] Daarnaast maken de meest geavanceerde systemen voor spraakherkenning het voor ontwikkelaars mogelijk om bepaalde voorkeuren in het systeem te verwerken, waaronder:

[10] IBM. *Speech Recognition*. (2021, 3 augustus). Geraadpleegd op 5 april 2022, van https://www.ibm.com/nl-en/cloud/learn/speech-recognition#toc-key-featur-DdHYi0BA.

- *Taalweging* (het verbeteren van de precisie van systemen door specifieke woorden die vaak voorkomen (bijvoorbeeld productnamen of vakjargon) een bepaalde weging te geven, naast termen die al in het lexicon zijn opgenomen).
- *Sprekerclustering* (het labelen van de bijdragen van elke individuele spreker in een gesprek met meerdere deelnemers).[11]
- *Akoestiektraining* (het trainen van het systeem om zich aan te passen aan de akoestische omgeving die het domein kenmerkt en de stijl waarop daarbinnen gesproken wordt (bijvoorbeeld toonhoogte, volume en tempo)).
- *Filtering van ongewenst taalgebruik* (het gebruik van filters om bepaalde ongewenste woorden of zinsdelen te identificeren en de spraakuitvoer te zuiveren).

Om spraak in geschreven tekst om te zetten en de accuraatheid daarvan te verbeteren, wordt gebruik gemaakt van een verscheidenheid aan algoritmen en wiskundige technieken. Hier vallen onder meer de volgende technieken onder:

- *Natural Language Processing* (hierna: 'NLP'): Hoewel NLP geen algoritme is dat een specifieke toepassing heeft binnen spraakherkenning, vormt het onderdeel van AI met een specifieke focus op de interactie tussen mens en machine middels taal, bestaande uit spraak en tekst. NLP doet een nadere classificatie van woorden en tekstonderdelen.
- *Hidden Markov Models* (hierna: 'HMM'): HMM maken het mogelijk om bepaalde verborgen en niet-observeerbare omstandigheden op te nemen in een probabilistisch model. Binnen het kader van spraakherkenning worden HMM gebruikt om als sequentiemodellen, waarbij labels aan elke eenheid worden toegewezen (woorden, lettergrepen, zinnen enzovoorts). Dit maakt het mogelijk om de meest geschikte volgorde van labels te bepalen. HMM worden in spraakherkenning gebruikt als statistische modellen van de akoestische eigenschappen van spraakklanken en delen daarvan.

[11] Sprekerclustering onderscheidt zich van sprekerherkenning omdat er geen individuele sprekers worden herkend. Bij sprekerclustering worden segmenten van de audio aangewezen als (waarschijnlijk) afkomstig van dezelfde spreker. Door elk van die clusters apart te normaliseren, kunnen betere spraakherkenningsscores worden bereikt.

- *N-grams*: N-grams zijn onderdelen van het taalmodel die kansen toekennen aan zinnen of zinsdelen. Grammatica en de waarschijnlijkheid dat bepaalde woordreeksen zich voordoen, worden gebruikt om de herkenningsnauwkeurigheid te optimaliseren.
- *Neurale netwerken*: Neurale netwerken worden met name gebruikt ten behoeve van zogeheten 'deep learning' algoritmes en verwerken trainingsdata door de interconnectiviteit van het menselijk brein voor zover bekend en mogelijk middels verschillende lagen en knooppunten na te bootsen.
- *Speaker Diarization* (hierna: 'SD'): Het SD algoritme maakt het mogelijk om spraak van verschillende sprekers te identificeren en te segmenteren. De sprekers worden niet als zodanig geïdentificeerd, maar de spraak wordt per spreker geclusterd. Hiermee is SD sterk verwant met spreker clustering.

2.2.2 Het proces van trainen en hertrainen

Voordat spraakherkenningssystemen gebruikt kunnen worden, moeten zij getrained worden. Dit gebeurt met behulp van trainingsdata. Deze trainingsdata kan bestaan uit ingesproken teksten, maar ook uit audio-opnamen of het audiokanaal van video-opnamen. Nadat het spraakherkenningsmodel met de nodige trainingsdata is gevoed, wordt de mate van accuraatheid van de spraakherkenningstechnologie geëvalueerd op basis van de gelijkenis met een onafhankelijke test.

Wanneer we kijken naar de toepassing van spraaktechnologie binnen het JenV-domein en de vraagstelling van dit rapport is het goed om aan te geven (in algemene zin) hoe het proces verloopt voor het trainen en gebruiken van een spraaktechnologie model.

2.2.2.1 Stap 1: Verzamelen trainingsdata

De eerste stap in het proces is het verzamelen van trainingsdata. Met deze data wordt het model getraind dat uiteindelijk menselijke spraak moet gaan herkennen.

2.2.2.2 Stap 2: trainen van het model

In de tweede stap van het proces wordt het model getraind. Dit betekent dat de trainingsdata wordt geprepareerd en door één of meer leer algoritmen wordt gehaald. De

ontwikkelaars van het model valideren en testen het meest geschikte model. Dit model is het 'eindproduct' dat wordt gebruikt om spraak te herkennen.

2.2.2.3 Stap 3: het in productie nemen en gebruiken van het model

In de derde stap wordt het model in productie genomen en vervolgens gebruikt. Dit betekent dat de gebruiker daadwerkelijke spraak (input data) door het model gaat laten herkennen.

2.2.2.4 Stap 4: Hertrainen van het model

Om het model beter te laten worden, kan het model opnieuw getraind worden. Dit betekent dat het model op basis van nieuwe data verder leert. Hierdoor wordt het model verder verfijnd.

2.2.3 Trainingsdata en beperkingen

In principe kunnen alle vormen van audio gebruikt worden om spraakherkenning te trainen, mits er een correcte transcriptie aan verbonden is. Zo kunnen naast audiofragmenten ook videobeelden (althans de afgestripte audiokanalen daarvan) gebruikt worden om spraakherkenning te trainen.

Training van spraakherkenning op basis van ingesproken teksten kent een aantal beperkingen. Zo zijn spraakherkenningssystemen die ontwikkeld worden aan de hand van voorgelezen teksten minder goed in staat om spraak in spontane gesprekken te herkennen en deze om te zetten in tekst, ondanks het feit dat dit de hoofdfunctie van spraakherkenning is. Omdat spontane gesprekken meer variabiliteit kennen dan voorgelezen teksten, is de spraakherkenning niet altijd volledig accuraat. Naast statische audiofragmenten is het daarom gebruikelijk om audiofragmenten van spontane gesprekken als trainingsdata te gebruiken bij de ontwikkeling van spraakherkenning. Zo wordt bij de ontwikkeling van spraakherkenning voor toepassing binnen de politie bijvoorbeeld gebruik gemaakt van verhoorgesprekken en gesprekken afkomstig uit de 112 meldkamer.

Daarnaast kan spraakherkenning over het algemeen gekwalificeerd worden als spreker-afhankelijk of spreker-onafhankelijk.[12] Spreker-afhankelijke spraakherkenning is getraind om spraaksignalen van een bepaalde spreker te herkennen, terwijl spreker-onafhankelijke spraakherkenning getraind is om spraaksignalen van groepen mensen te herkennen. Belangrijk om hierbij te vermelden is dat spreker-afhankelijke spraakherkenning minder variabiliteit kent dan spreker-onafhankelijke spraakherkenning. Spreker-afhankelijke spraakherkenning is getraind met behulp van de spraakdata van een bepaalde persoon, waardoor de variabiliteit in de uitspraak van woorden relatief beperkt is – deze varieert slechts beperkt door verandering in onder meer emotie of lichamelijke conditie. Omdat spreker-onafhankelijke spraakherkenning getraind is op spraakdata van (vele) verschillende personen, kent deze een grotere variabiliteit. De aanpak van deze variabiliteit vormt de grootste uitdaging voor spraakherkenning. Daarnaast is het belangrijk dat de trainingsdata niet gelijktijdig kan worden gebruikt voor training en testen – wanneer dit wel wordt gedaan, is het mogelijk dat het systeem disproportioneel veel getraind is om de trainingsdata te herkennen en onvoldoende of helemaal niet meer in staat is om op variaties daarin in de input data te reageren. Wanneer er weinig of geen gelijkenis bestaat tussen beide (in een dergelijk geval is de accuraatheid laag), spreken we van een zogeheten '*mismatch problem*'. Om dit probleem te voorkomen, is het van belang dat spraakherkenningssystemen met voldoende trainingsdata worden gevoed en dat een representatief trainingsalgoritme wordt ontwikkeld.

2.3 Algemene toepassingen

Tot de vroegste toepassingen voor spraakherkenning behoren geautomatiseerde telefoonsystemen en medische dicteersoftware. Tegenwoordig wordt spraakherkenning voornamelijk gebruikt voor het dicteren van opgenomen spraak, het doorzoeken van databases en het geven van opdrachten aan computersystemen. Vandaag de dag maakt een groot aantal industrieën gebruik van verschillende toepassingen van spraakherkenning, waaronder de auto-industrie, de gezondheidszorg, beveiliging en customer support.

[12] Idem.

3 Toepassing spraakherkenning binnen Justitie en Veiligheid

Spraakherkenning kan binnen verschillende organisaties binnen het JenV-domein worden ingezet. Om de onderzoeksvragen die in dit rapport centraal staan te kunnen beantwoorden is het van belang een beeld te vormen van huidige en toekomstige toepassingen van spraakherkenning binnen het JenV-domein. In dit hoofdstuk worden drie *use cases* binnen het JenV-domein beschreven die illustreren hoe spraakherkenning in de toekomst kan worden ingezet.

We bespreken de inzet van spraakherkenning bij de Nationale Politie, de Reclassering en een fictieve organisatie binnen het JenV-domein aan de hand van de interviews die binnen deze domeinen zijn afgenomen.[13] Er is gekozen voor deze drie *use cases* omdat ze ieder binnen een ander privacyrechtelijk kader vallen (AVG, Wpg en de Wjsg). Dit stelt ons in staat om juridische vraagstukken vanuit deze verschillende wettelijke kaders te beschouwen.

In dit hoofdstuk staan we daarnaast stil bij een aantal praktische gevolgen van de inzet van spraakherkenning binnen de gegeven *use cases*. In hoofdstuk 5 vestigen we vervolgens de aandacht op de (juridische) risico's van de toepassing van spraakherkenning binnen elk van de besproken *use cases* en mogelijke maatregelen voor het mitigeren van deze risico's.[14]

3.1 Politie

Binnen de Nationale Politie (hierna ook: 'de politie') worden de mogelijkheden van spraaktechnologie onderzocht. Naar aanleiding van een aantal experimenten met

[13] Omdat er geen casus beschikbaar was voor deze laatste *use case* wordt gebruik gemaakt van een representatieve fictieve casus. De organisatie die in deze fictieve casus wordt beschreven staat model voor verschillende organisaties binnen het JenV-domein. Binnen de *use case* van de Nationale Politie wordt onderscheid gemaakt tussen drie proeftuinen.

[14] In dit rapport wordt een bredere juridische analyse geboden van de ontwikkeling en toepassing van spraakherkenning binnen het JenV-domein. Om de juridische kwesties die hierbij om de hoek komen kijken zo goed mogelijk in kaart te brengen, is ervoor gekozen een juridische analyse uit te voeren aan de hand van drie *use cases*: politie, Reclassering en een JenV instantie in het Wjsg-domein. De eerste twee *use cases* zijn gebaseerd op huidige onderzoek binnen JenV terwijl de laatste *use case* een fictieve casus is ter illustratie van een mogelijke toepassing van spraakherkenning binnen JenV in de toekomst.

spraaktechnologie is de politie overgegaan tot de ontwikkeling van een Generieke Dienst Automatische spraakverwerking (hierna: 'GDAS').

Het programma GDAS ontwikkelt een voorziening waarmee op termijn verschillende vormen van spraaktechnologie mogelijk worden gemaakt. Voorbeelden hiervan zijn:

Automatische spraakherkenning waarbij spraak automatisch wordt herkend en omgezet naar tekst (spraakherkenning).	Binnen scope van het onderzoek van Considerati.
Het onderscheiden van verschillende sprekers in een groep (*speaker diarization*).	Buiten scope van het onderzoek van Considerati.
Sprekerherkenning (*speaker recognition*).	Buiten scope van het onderzoek van Considerati.

Het programma GDAS heeft drie toepassingen (proeftuinen) benoemd binnen verschillende domeinen van de politie waarbinnen spraakherkenning kan worden ingezet. De volgende drie toepassingen worden in dit rapport nader uitgewerkt:

- verhoren binnen het domein van opsporing;
- het maken van notities bij handhaving (het digitaal gesproken zakboekje)[15]; en
- meldingen binnen het domein van het Operationeel Centrum (hierna: 'OC') (112-meldingen politie).

In het navolgende beschrijven we per proeftuin welke rol spraakherkenning daarbinnen speelt. Hierbij zoomen we ook in op een aantal gevolgen van de inzet van spraakherkenning voor zowel de politie alsook de betrokkenen[16,17]

[15] Inmiddels wordt hierbij ook breder gekeken naar toepassingen binnen het domein van de Gebiedsgebonden Politie (hierna: 'GGP').
[16] Een betrokkene is een geïdentificeerde of identificeerbare natuurlijke persoon van wie persoonsgegevens worden verwerkt.
[17] De verwachte gevolgen de wij in dit onderzoek beschrijven zijn aan het licht gekomen tijdens het brononderzoek van de door de politie aangeleverde stukken en interviews die Considerati met stakeholders van de politie heeft gehouden. Het

3.1.1 Use case(s)

3.1.1.1 Verhoor

Beschrijving

Een van de spraak-naar-tekst-applicaties van de GDAS is ten behoeve van verhoren en richt zich er met name op om de werkdruk te verlagen.[18] Dit gebeurt bijvoorbeeld bij audiovisuele registratie verhoor (hierna: 'AVR'). In bepaalde zaken wordt het verhoor auditief of audiovisueel geregistreerd, wat betekent dat het verhoor wordt opgenomen (geluid of beeld en geluid).[19] Dit is bijvoorbeeld het geval bij verhoren van kwetsbare verdachten (VKV). Hoewel de woordelijke uitwerking van deze verhoren momenteel nog handmatig gebeurt[20], biedt spraakherkenning de mogelijkheid om automatisch een transcriptie te laten plaatsvinden. Tot slot zou spraakherkenning ingezet kunnen worden bij veelvoorkomende criminaliteit (VVC).[21] De huidige werkwijze bij VVC-verhoren is dat tijdens de verhoren voornamelijk wordt meegetypt en het verhoor niet of nauwelijks wordt opgenomen. Omdat meetypen als afleidend wordt ervaren, is het de wens om in de plaats hiervan in de toekomst spraakherkenning in te zetten.[22]

Gevolgen: voor- en nadelen

Spraakherkenning bij verhoren van de politie kent verschillende voordelen, waaronder:

- *Minder druk op operationele beschikbaarheid politie*

verdient hierbij opmerking dat de beschreven voordelen en/of implicaties niet uitputtend zijn en louter dienen als voorbeeld om het belang van spraakherkenning aan te tonen.

[18] De hoop en het uitgangspunt is dat de politie voor verschillende toepassingen kunnen volstaan met één applicatie met wellicht verschillende opties. Verhoor loopt op de troepen vooruit, omdat de politie hier de beste beschikbaarheid had van medewerkers en omdat verhoor een afgebakend geheel is waarbij het evident is dat ASR een noodzakelijk vervolgstap is ten behoeve van het opstellen van het proces-verbaal.

[19] De politie heeft in sommige gevallen de verplichting en in andere gevallen de keuze om verhoren auditief of audiovisueel op te nemen, afhankelijk van de aard van het misdrijf (zware criminaliteit, zeden) of de persoon die gehoord wordt (minderjarige verdachten of kwetsbare verdachten).

[20] Het handmatig omzetten van spraak naar tekst wordt handmatig gedaan door de rechercheurs, of door het verhoor op te sturen naar gespecialiseerde schrijftolken die door de politie worden ingehuurd.

[21] Met veelvoorkomende criminaliteit worden strafzaken bedoeld die vaak voorkomen en binnen een relatief kort termijn worden afgehandeld zoals winkeldiefstal, vandalisme en uitgaansgeweld.

[22] In het kader van de Modernisering Wetboek van Strafvordering, waarbij auditieve en audiovisuele registraties als zelfstandig bewijsmiddel mogen worden ingediend, zal er waarschijnlijk meer worden opgenomen bij het VVC. De Innovatiewet Strafvordering gaat deze mogelijkheid beproeven. We bespreken beide nader in hoofdstuk 5.2.

Bij de huidige werkwijze van de politie worden audiovisuele verhoren achteraf handmatig getranscribeerd. Deze taak neemt veel tijd in beslag en legt daardoor druk op de operationele beschikbaarheid van politiemedewerkers. Daarnaast is het laten transcriberen erg kostbaar. Inzet van spraakherkenning vermindert de administratieve last aangezien de opname van het verhoor automatisch wordt getranscribeerd. Verder zorgt spraakherkenning ervoor dat politiemedewerkers zich kunnen focussen op hun primaire werkzaamheden.

- *De voortgang van het onderzoek verbetert*

  Spraakherkenning zorgt er waarschijnlijk voor dat de tekstuele uitwerking van het verhoor sneller beschikbaar is waardoor het opsporingsonderzoek effectiever kan worden uitgevoerd. Dit is in het belang van de politie en van de verdachte. Omdat er nog weinig getest is om te weten of een automatische transcriptie even goed of sneller beschikbaar is, is nader onderzoek nodig.

- *De kwaliteit van het verhoor verbetert*

  Doordat het verhoor wordt opgenomen en er niet meer wordt meegetypt is er tijdens het verhoor meer aandacht voor de verdachte en neemt het verhoor meer de vorm aan van een interview. Uit onderzoek[23] is gebleken dat dit bijdraagt aan de kwaliteit en betrouwbaarheid van het verhoor. Wanneer het verhoor automatisch wordt getranscribeerd zorgt dit er bovendien voor dat er minder ongewenste pauzes zijn waardoor het verhoor meer organisch verloopt.

- *Gebruik in de strafrechtketen*

  In het kader van de modernisering Wetboek van Strafvordering wordt het expliciet wettelijk mogelijk gemaakt om audiobestanden als wettelijk bewijsmateriaal toe te laten in de strafrechtketen. Hiermee wordt deze mogelijkheid aan de limitatieve opsomming van toelaatbaar bewijsmateriaal uit artikel 339 Sv toegevoegd, hoewel

[23] Geijsen, (2019), Kwetsbare verdachten tijdens het politieverhoor. Ars Aequi. https://arsaequi.nl/product/kwetsbare-verdachten-tijdens-het-politieverhoor.

er hierdoor in juridische zin geen specifieke veranderingen teweeg worden gebracht. Specifieke regels omtrent het gebruik van het desbetreffende materiaal worden in de wet echter niet gegeven, zolang de beelden of geluiden die als bewijs worden gebruikt persoonlijk en op het onderzoek ter terechtzitting door de rechter zijn waargenomen. Hoewel een schriftelijke transcriptie hiertoe niet vereist is, is het aannemelijk dat de vraag naar spraakherkenning door de modernisering Wetboek van Strafvordering toeneem omdat men mogelijk naast het audiobestand ook een transcriptie aan de rechter wil voorleggen.

- *De informatiepositie van de politie verbetert*

  Zoals uit het voorgaande blijkt, worden momenteel worden niet alle verhoren van de politie standaard opgenomen. Hierdoor is het mogelijk dat er informatie verloren gaat. Wanneer het verhoor wordt opgenomen en automatisch in tekst wordt vastgelegd, verbetert dit mogelijk de informatiepositie van de politie. Tekst is namelijk beter/makkelijker te doorzoeken of analyseren dan audio. Daarnaast geldt dat omdat hierbij steeds de letterlijke tekst wordt gebruikt, interpretatie of parafrasering niet voorkomt en informatie dus minder snel verloren gaat.

- *Psychologisch effect gedrag verdachte*

  Inzet van spraakherkenning kan mogelijk een psychologisch effect hebben op het gedrag van de verdachte. Uit communicatie met politie is gebleken dat intern onderzoek laat zien dat de verdachte door de gesprekssnelheid of druk minder tijd heeft om zijn gedachten te vormen of antwoorden te bedenken. Dit kan voordelig zijn voor de voortang van het onderzoek, hoewel de daadwerkelijke impact hiervan verder onderzocht zal moeten worden.

- *Context kan mogelijk beter in kaart gebracht worden*

  Doordat een agent bij de toepassing van spraakherkenning in de gelegenheid wordt gesteld om meer aandacht aan de verdachte te besteden, met name bij VCC-verhoren, wordt het voor hem mogelijk om meer op non-verbaal gedrag van de

verdachte te letten. Zo is het bij spraakherkenning eenvoudiger om steeds (oog)contact met verdachte te hebben. Daarnaast kunnen gesignaleerde emoties of gedragingen door de verhoorder benoemd worden (bijv. 'ik zie dat je boos/verdrietig/blij wordt'), waardoor dit ook in de transcriptie wordt opgenomen.

- *Rechtsbescherming en waarheidsvinding verbetert*

  Tenslotte is een belangrijk potentieel voordeel dat tijdens het onderzoek ter terechtzitting de rechter niet alleen hoeft te varen op een verslag van een audio opname en de audio opname zelf. Met de invoering van de Innovatiewet Strafvordering is het toegestaan om audio en video op te nemen in het dossier (in plaats van een volledig uitgeschreven proces verbaal). Het is goed mogelijk dat audio opnamen voor de rechter en de verdediging minder eenvoudig toegankelijk zijn dan een proces verbaal (al is het alleen maar omdat lezen doorgaans sneller gaat dan luisteren). Hierdoor ontstaat het risico dat zowel rechter als verdediging om tijd te besparen varen op het verkorte verslag, hetgeen afbreuk kan doen aan de waarheidsvinding en de rechtsbescherming voor de verdachte. Door het toevoegen van een transcript wordt dit risico verkleind.

Nadelen bij deze toepassing zijn mogelijk:

- *Psychologisch effect gedrag verdachte*

  Inzet van spraakherkenning kan mogelijk een psychologisch effect hebben op het gedrag van de verdachte. Het is bijvoorbeeld mogelijk dat de verdachte zich onder druk voelt staan en bepaalde zaken achterwege laat of niet vertelt omdat het gesprek wordt opgenomen. Dit kan nadelig zijn voor het onderzoek.

- *Context gaat mogelijk verloren*

  Er gaat mogelijk informatie verloren, waar emoties niet door een agent worden opgemerkt en daardoor niet in de transcripties worden opgenomen. Emoties worden namelijk niet gedetecteerd en daarbij automatisch genoteerd bij spraakherkenning. Hierdoor kan misschien context in het gesprek verloren gaan.

- *Informatie gaat verloren*

  Hoewel de inzet van spraakherkenning de informatiepositie van de positie kan verbeteren bij her uitvoeren van verhoren, kan het letterlijk uitwerken van verhoren er ook voor zorgen dat informatie praktisch gezien verloren gaat. Zo is spraakherkenning niet vrij van fouten en bestaat de kans dat de leesbaarheid potentieel slechter wordt. Het gevolg hiervan is het moeilijker wordt om de juiste informatie uit de transcriptie te halen.

3.1.1.2 Digitaal gesproken zakboekje

Beschrijving

Een andere spraak-naar-tekst-applicatie van de GDAS is richt zich op de inzet van deze technologie binnen de GGP. De toepassing van spraakherkenning binnen de GGP wordt het digitaal "gesproken" zakboekje genoemd en heeft tot doel het proces van het maken van aantekeningen en notities door medewerkers van de GGP te automatiseren.[24] De medewerker van de politie die het digitaal gesproken zakboekje gebruikt[25] kan zijn observaties, nog uit te voeren acties en aantekeningen via een mobiele applicatie inspreken waarna het door middel van de spraak-naar-tekst-app[26] automatisch wordt omgezet in een tekstbestand.

Dit maakt het voor een GGP-agent makkelijker om zijn bevindingen en observaties in te spreken en om te zetten naar tekst. Ook kan de agent aantekeningen maken tijdens het rijden zonder bijrijder.

[24] Momenteel verkeert de politie nog in de ontwikkelfase van spraakherkenning en zijn er nog geen operationele testen gedaan. Hierdoor is het momenteel nog onduidelijk welk type apparaat het best voor het digitaal zakboekje wordt gebruikt. Dit wordt mede ingegeven door de omstandigheden waarin deze opname plaatsvindt. Als dat in onverwachte en/of hectische omstandigheden geschieden is het volgens de politie nog maar de vraag welk type apparaat het best geschikt is om een opname te maken.
[25] In de praktijk zijn dit veelal (niet uitsluitend) de medewerkers binnen de politie die voor een belangrijk deel hun werk 'op straat' verrichten. Denk hierbij aan wijkagenten/buurtregisseurs en de surveillance, c.q. nooddiensten.
[26] Dit betreft naar alle waarschijnlijkheid dezelfde applicatie als die binnen het kader van het verhoor wordt ingezet.

Tot slot kan het digitaal gesproken zakboekje gebruikt worden om gesprekken met mensen op straat (getuigen, slachtoffers, een gesprek met een straathoekmedewerker etc.) op te nemen en deze automatisch te transcriberen.

Gevolgen: voor- en nadelen[27]

Spraakherkenning bij GGP brengt naar verwachting onder meer de volgende voordelen met zich mee:[28]

Versterkt informatiepositie van teams

Doordat de ingesproken aantekeningen automatisch in tekst worden omgezet, is het mogelijk om sneller meer informatie vast te leggen in de registratiesystemen. Dit zorgt ervoor dat informatie sneller beschikbaar is en verbetert de informatiepositie van de politie.

(Near) realtime delen informatie met backoffice

In plaats van bellen, kan de medewerker van de politie de transcriptie van zijn gesproken notities doorsturen naar de backoffice. Hierdoor beschikt de backoffice snel over de informatie op schrift. De backoffice medewerker hoeft daardoor niet meer zelf aan de telefoon mee te luisteren en vragen te stellen, waardoor minder informatie verloren gaat en sneller gehandeld kan worden.

3.1.1.3 Operationeel Centrum 112-meldkamer

Beschrijving

De politie wil spraakherkenning ook gebruiken om 112-meldingen in de meldkamer automatisch om te zetten in tekst. Het deel van de meldkamer waar meldingen gericht aan de politie binnenkomen wordt het 'operationeel centrum' genoemd. De huidige werkwijze binnen het operationeel centrum houdt in dat de centralist tijdens het gesprek met de melder aantekeningen maakt en informatie registreert in het daarvoor bestemde systeem.

[27] Aangezien de politie momenteel nog in de ontwikkelingsfase ontwikkelfase van spraakherkenning verkeert, is het mogelijk dat er op termijn aanvullende voor- en nadelen zullen worden geïdentificeerd met betrekking tot het digitaal gesproken zakboekje.
[28] Zie de memo "ontheffingsverzoek gebruik productiedata bij de ontwikkeling van GDAS en S2T" van de politie.

De politie wil spraakherkenning door middel van real time transcriptie inzetten zodat de centralist zich meer kan richten op de beller en zich minder hoeft te focussen op het invoeren van de melding in het meldkamersysteem. Met real time transcriptie wordt bedoeld dat de spraak live wordt omgezet in tekst en dit dus niet achteraf gebeurt.

Gevolgen: voor- en nadelen

De voordelen die spraakherkenning teweegbrengt zijn als volgt:

- *Centralist kan zich focussen op het gesprek met de melder*

  Door een *real time* transcriptie hoeft de centralist zelf minder aandacht te besteden aan het invoeren van de melding in het meldkamersysteem tijdens het contact met de beller. Er kan beter geluisterd worden, meer empathie worden getoond, en meer worden uitgevraagd.

- *Verbetering informatiepositie RTIC[29] en eenheden*

  Door de tekst real time beschikbaar te stellen aan het RTIC, beschikt de informatiemedewerker over de informatie zoals die exact door de melder is doorgegeven. Dit vormt de basis voor veredelen[30] van de melding. Doordat de centralist niet meer gelijktijdig hoeft te luisteren en mee typen, gaat er geen informatie verloren tussen de melder en de informatiemedewerker. Ook voor de surveillance of noodhulp geldt dat wanneer de centralist de tekst van het gesprek real time deelt met de dienstvoertuigen, deze medewerkers direct over de exacte informatie beschikken die van de melder afkomstig is.

- *Kwaliteitsmanagement*

  Door de beschikbaarheid van de exacte transcriptie van de meldingen kan deze informatie - binnen de grenzen van de AVG en andere wetten – worden gebruikt voor kwaliteitsmanagementdoeleinden.

[29] RTIC staat voor het Real-Time Intelligence Center. Het RTIC is gepositioneerd op de meldkamer en levert een bijdrage aan het aansturen van politieoperaties.
[30] Met het veredelen van informatie houdt in dat gegevens worden gecontroleerd, hiaten worden aangevuld en tegenstrijdigheden worden verwijderd.

Bij deze toepassing signaleren we ook een specifiek nadeel:

- *Real time transcriptie gevoeliger voor fouten*
  Het gebruik van automatische spraak naar tekst in de meldkamer is alleen bruikbaar als dit real time gebeurt omdat de informatie vanwege het spoedeisende belang direct beschikbaar moet zijn. Afhankelijk van de kwaliteit van he spraakmodel, is de kans op fouten mogelijk groter. De consequenties van fouten zijn potentieel groter, met name waar de fouten storend zijn voor de strekking van de inhoud, omdat er direct geacteerd moet worden en er geen tijd is om achteraf fouten te herstellen. Wanneer bijvoorbeeld een adres verkeerd getranscribeerd wordt en de centralist heeft het adres ook niet genoteerd, dan kan dit bovendien consequenties hebben voor de hulpverlening.

3.1.2 Technische werking GDAS

GDAS is door de politie geïntroduceerd met het doel om spraaktechnologie breed binnen de politie beschikbaar te stellen. De ambitie hierbij is om altijd de best mogelijke kwaliteit te leveren. Het zelf ontwikkelen van een spraakmodel dat is toegesneden op de politiepraktijk kan hieraan bijdragen. Momenteel worden in de ontwikkeling van dit spraakmodel twee componenten onderscheiden: het akoestisch model (het model dat geluidsgolven omzet in klanken) en het lexicon (de lijst met woorden die door de technologie herkend kunnen worden).

Om de hierboven genoemde modellen te gebruiken in specifieke gevallen worden ze getraind op corpora. Dit zijn sets met soms generieke en soms heel specifieke data, bestaande uit een audiofragment en de daarbij horende transcriptie (voor het akoestisch model) of tekst (voor het taalmodel/lexicon). Wanneer de toepassing van de spraakherkenner geluid is met een specifiek karakter, zoals een opname in een verhoorstudio, dan is het van belang een corpus met passend zuiver audiofragment en bijhorende transcriptie te verzamelen. Het trainen met specifieke data gebeurt meestal om

de performance van het spraakherkenningsmodel te optimaliseren. Het is niet per se zo dat elke toepassing van deze technologie een eigen model vergt. Soms zijn generieke modellen al voldoende en soms dient de specifieke data om het generieke model in algemene zin te verbeteren. Als de toepassing een specifiek onderwerp betreft, bijvoorbeeld gebruik van spraakherkenning tijdens politieverhoren, is het van belang dat een corpus met een passende tekst wordt gebruikt.

Akoestisch model

Het toepassen van spraak naar tekst bij 112-meldingen kent specifieke uitdagingen. Zo is de kwaliteit van de audio doorgaans minder (zware compressie, lage bandbreedte, sprekers staat op straat, spreker is emotioneel/verward et cetera). Voor de ontwikkeling van GDAS is een kleine set materiaal uit een ander project met 112 gebruikt om het akoestisch model te optimaliseren. Dit levert een goede verbetering, maar meer data levert naar verwachting een beter model op.

Opnames (op straat) voor het digitale zakboekje zullen naar verwachting (door de kwaliteiten van de gebruikte telefoons) relatief schoon zijn. Het is op dit moment nog niet duidelijk of het nodig is om voor de bruikbaarheid van dit model voor deze proeftuin specifieke data te verzamelen. In dit geval weet de spreker (de medewerker van de politie die de toepassing gebruikt) dat er spraakherkenning wordt ingezet en heeft deze belang bij de nauwkeurigheid en kwaliteit van de opname.

Concluderend is er voor het gebruik van spraakherkenning bij 112-meldingen een specifiek akoestisch model nodig, waarvoor al een eerste versie bestaat. Voor het digitale zakboekje moet worden uitgezocht of een specifiek akoestisch model noodzakelijk is. Hierbij kijkt de politie met name naar de performance die behaald kan worden met de modellen die zij tot haar beschikking heeft, waarbij verder beoordeeld wordt in hoeverre er ruimte voor verbetering is middels training met eigen data.

Taalmodel

De inhoud van 112-meldingen en het digitale zakboekje is anders dan de inhoud van verhoren die in beginsel gelden als trainingsdata waar het spraakmodel van GDAS op gebaseerd is. Het onderwerp van de verschillende politietoepassingen is weliswaar onderling verschillend, maar er zijn veel overeenkomsten. De grootste winst zal naar waarschijnlijkheid gehaald worden met het ontwikkelen van een 'breed' politiemodel dat voor de verschillende toepassingen ingezet kan worden. Naar verwachting dient dit model versterkt te worden met modellen voor specifieke onderwerpen, indien hier geschikte tekstcorpora voor beschikbaar zijn.

3.2 Reclassering

3.2.1 Introductie

Naast de politie onderzoekt ook de Reclassering Nederland (hierna: de Reclassering) de toepassing van spraakherkenning. De Reclassering heeft een wettelijke taak waaronder advisering aan rechters, officieren van justitie en gevangenisdirecteuren over verdachten en veroordeelden: de reclassenten. Zij houdt toezicht op hen, geeft gedragstrainingen en begeleidt hen bij de uitvoering van een werkstraf (ook de organisatie van de werkstraf zelf is een taak van de reclassering).[31] Hieronder wordt beschreven wanneer en hoe spraakherkenning de Reclassering kan helpen met het uitvoeren van haar taken.

3.2.2 Use case(s)

In het onderzoek naar de bruikbaarheid van spraakherkenning binnen de Reclassering heeft Rene Poort, strategisch adviseur Reclassering Nederland, een verkennend onderzoek gedaan. Hierin maakt hij onderscheid tussen eenvoudige spraakherkenning en uitgebreide spraakherkenning. In dit onderzoek beperken wij ons tot het automatisch omzetten van spraak naar tekst (eenvoudige spraakherkenning).

Eenvoudige spraakherkenning: een technologie die op basis van AI spraak automatisch omzet in geschreven tekst.	Binnen scope van het onderzoek van Considerati

[31] Deze tekst is een parafrase van de tekst op de website van Reclassering Nederland: https://www.reclassering.nl/over-de-reclassering/wat-wij-doen. Geraadpleegd op 27 oktober 2022.

Uitgebreide spraakherkenning: een technologie die op basis van AI data uit gesproken tekst haalt, analyseert en op basis hiervan conclusies trekt of voorstellen doet.	Buiten scope van het onderzoek van Considerati

Beschrijving

Medewerkers van de Reclassering voeren veel gesprekken met onder andere verdachten en daders. De huidige werkwijze houdt in dat de medewerker hiervan aantekeningen maakt. Spraakherkenning kan ervoor zorgen dat de gesprekken die de reclasseringswerker voert automatisch worden getranscribeerd. Daarnaast biedt spraakherkenning naar verwachting een uitkomst bij het schrijven van adviesrapporten. Wanneer gebruik wordt gemaakt van spraakherkenning kunnen medewerkers van de Reclassering een advies inspreken dat vervolgens automatisch wordt omgezet in een tekstbestand.

Gevolgen: voor- en nadelen

Spraakherkenning kent naar verwachting verschillende voordelen voor de Reclassing, waaronder:

- *Minder druk op de beschikbaarheid van de reclasseringswerker.*
  De huidige werkwijze houdt in dat de reclasseringswerker verslagen, rapporten en adviezen handmatig uittypt. Deze taak neemt veel tijd in beslag en legt daardoor druk op de beschikbaarheid van de reclasseringswerker. Hierdoor kan de reclasseringswerker een hoge administratieve last ervaren. Daarnaast is het laten transcriberen erg kostbaar. Inzet van spraakherkenning vermindert de administratieve last aangezien gesprekken opgenomen worden en automatisch worden getranscribeerd. Dit zorgt ervoor dat reclasseringswerkers zich kan richten op de primaire taken.

- *Uitwerking van een gesprek is sneller beschikbaar*

  Spraakherkenning zorgt er mogelijk voor dat de tekstuele uitwerking van het gesprek tussen de reclassant en de reclasseringswerker sneller beschikbaar is. Hierdoor kan er binnen een korter tijdsbestek en advies voor de rechterlijke macht worden opgesteld.

- *De kwaliteit van de gesprekken verbetert*

  Wanneer gesprekken tussen de reclasseringswerker en de reclassant worden opgenomen en automatisch worden getranscribeerd, kan de reclasseringswerker zich beter richten op de reclassant omdat hij/zij geen aantekeningen meer hoeft te maken. Hierdoor kan beter geluisterd worden, meer empathie worden getoond, en meer worden uitgevraagd. Dit komt de kwaliteit van het gesprek ten goede.

- *De informatiepositie van de Reclassering verbetert*

  Momenteel maakt een reclasseringswerker uitsluitend aantekeningen tijdens het gesprek met de reclassant waardoor er mogelijk informatie verloren gaat omdat de reclasseringswerker niet het gehele gesprek kan meeschrijven. Wanneer gesprekken tussen de reclasseringswerker en de reclassant worden opgenomen en automatisch omgezet in tekst, is er naar verwachting een completer verslag van het gesprek. Dit heeft een positieve impact op de informatiepositie van de Reclassering. Tekst is namelijk beter/makkelijker te doorzoeken of analyseren dan audio. Daarnaast geldt dat omdat hierbij steeds de letterlijke tekst wordt gebruikt, interpretatie of parafrasering niet voorkomt en informatie dus minder snel verloren gaat.

- *Non-verbaal gedrag kan mogelijk beter in kaart gebracht worden*

  Omdat de medewerker door spraakherkenning meer aandacht aan de reclassant kan besteden, kan beter op non-verbale communicatie worden gelet. Zo is het bij spraakherkenning eenvoudiger om steeds (oog)contact met reclassant te hebben. Daarnaast kunnen gesignaleerde emoties of gedragingen door de

reclasseringswerker benoemd worden (bijv. 'ik zie dat je boos/verdrietig/blij wordt'), waardoor dit ook in de transcriptie wordt opgenomen.

Nadelen bij deze toepassing zijn mogelijk:

- *Psychologisch effect gedrag reclassant*
  Inzet van spraakherkenning kan een psychologisch effect hebben op het gedrag van de reclassant. Het is bijvoorbeeld mogelijk dat de reclassant zich onder druk voelt staan en bepaalde zaken achterwege laat of niet vertelt omdat het gesprek wordt opgenomen en volledig wordt getranscribeerd.

- *Context gaat mogelijk verloren*
  Er gaat mogelijk informatie verloren. Zo worden emoties niet gedetecteerd en getranscribeerd bij spraakherkenning. Hierdoor kan misschien context in het gespreksverslag verloren gaan als de emoties niet expliciet worden benoemd.

- *Informatie gaat verloren*
  Hoewel de inzet van spraakherkenning de informatiepositie van de Reclassering kan verbeteren bij het uitvoeren van gesprekken met de reclassant, kan het er ook voor zorgen dat informatie verloren gaat. Zo is spraakherkenning niet vrij van fouten en bestaat de kans dat de leesbaarheid potentieel slechter wordt. Het gevolg hiervan is het moeilijker wordt om de juiste informatie uit de transcriptie te halen.

3.3 Fictieve JenV-organisatie

3.3.1 Beschrijving

In aanvulling op de hierboven beschreven *use cases* wordt de inzet van spraakherkenning onderzocht aan de hand van een fictieve casus binnen het justitiedomein. De organisatie in deze casus kan model staan voor diverse organisaties zoals de IND, de Rechtspraak, Raad voor de Kinderbescherming, het OM, de DJI en de Dienst Justis. Gekozen is om een fictieve casus binnen het justitie-domein te introduceren om zo ook de randvoorwaarden die de Wjsg stelt aan de toepassing van spraakherkenning binnen JenV aan bod te laten komen.

3.3.2 Use case(s)

De fictieve instantie in het justitiedomein gebruikt spraakherkenning tijdens bijenkomsten met meerdere personen, zowel burgers als medewerkers. Op basis van inzichten verkregen uit de bijeenkomst en schriftelijke documentatie, wordt na afloop van de bijenkomst een besluit genomen dat rechtsgevolgen heeft voor de betrokken burger(s). Spraakherkenning wordt gebruikt ten behoeve van verslaglegging van de bijeenkomst. Daarnaast wordt spraakherkenning in deze fictieve casus ook toegepast in vergaderingen tussen medewerkers. Een medewerker van de fictieve instantie in het justitiedomein controleert het transcript en stelt op basis hiervan een verslag op. Bij de toepassing van spraakherkenning maakt de JenV organisatie gebruik van de producten en diensten van een commerciële leverancier.[32]

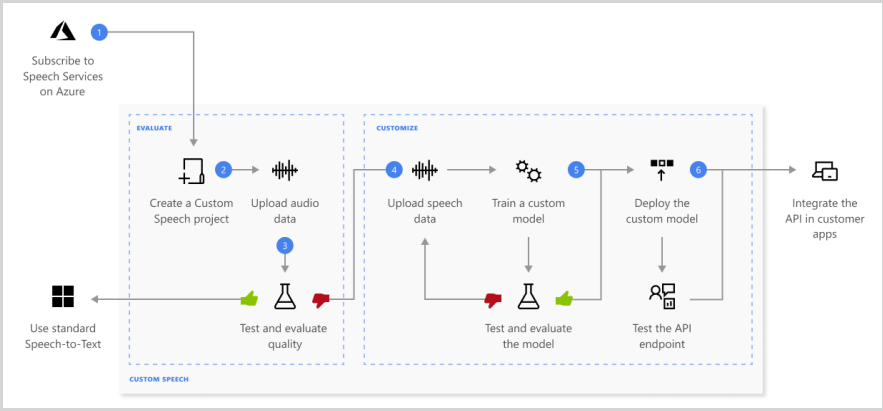
Voorbeeld

Een voorbeeld van een commerciële leverancier van software voor spraakherkenning en cloudtechnologie is Azure Cognitive Services van Microsoft. Azure Cognitive Services zijn cloudservices waarmee door middel van AI cognitieve intelligentie kan worden ingebouwd in toepassingen. Een onderdeel van deze dienst van Microsoft is de functie spraak naar tekst, waarmee audiobestanden getranscribeerd kunnen worden. Microsoft Azure maakt gebruik van een Universal Language Model als basismodel dat is getraind

[32] Een voorbeeld van een dergelijke commerciële leverancier wordt in het tekstblok onder aan de pagina gegeven. Dit voorbeeld betreft Microsoft Azure Cognitive Services. De gekozen leverancier dient enkel ter illustratie van de fictieve casus waar dit in het kader van dit rapport relevant is. Deze commerciële leverancier is als voorbeeld in dit rapport opgenomen gezien de complexiteit van de casus (niet-Nederlandse aanbieder, eventuele buitenlandse dataopslag en mogelijke vereisten op grond van de US Cloud Act).

met trainingsdata van Microsoft op basis van veelgebruikte gesproken taal. Microsoft stelt zelf dat dit model goed werkt in uiteenlopende scenario's omdat het is getraind met dialecten en fonetiek die in verschillende disciplines worden gebruikt.

Daarnaast biedt Microsoft de mogelijkheid om het basismodel aan te passen door het te voeden met specifieke audiofragmenten en bijhorende transcripties. Microsoft noemt dit *Custom Speech*. Waar JenV zou besluiten gebruik te maken van de spraakherkenningstechnologie van Microsoft, zou het basismodel naar alle waarschijnlijkheid niet voldoende aansluiten waar de technologie wordt ingezet in organisatie-specifieke gevallen (bijvoorbeeld vanwege specifiek jargon). De mogelijkheid die Microsoft biedt om het basismodel verder te ontwikkelen, maakt het model ook bruikbaar in organisatie-specifieke gevallen, waaronder ook voor JenV. In de afbeelding hieronder wordt weergegeven hoe organisaties zoals JenV het basismodel van Microsoft Azure kunnen aanpassen.



Afbeelding 4. *Proces van customizing* in Microsoft Azure Congnitive Services.

3.3.3 Gevolgen: voor- en nadelen

In de fictieve casus heeft spraakherkenning naar verwachting de volgende voordelen voor de organisatie:

- *Minder administratieve lasten*

Wanneer audiofragmenten van vergaderingen en bijeenkomsten door middel van spraakherkenning worden omgezet in tekst vermindert dit de administratieve lasten van medewerkers. Medewerkers hoeven notulen van vergaderingen en/of bijeenkomsten nu immers niet meer uit te typen.

- *Het verslag van de vergadering is completer*
  Wanneer vergaderingen of bijeenkomsten worden opgenomen en automatisch worden getranscribeerd door middel van spraakherkenning is het verslag naar verwachting completer. Een notulist die meeschrijft of typt kan nooit de volledige inhoud van de vergadering meenemen, wanneer audio automatisch wordt omgezet in tekst zorgt dit voor een volledig en compleet verslag van de vergadering.

Nadelen bij deze toepassing zijn mogelijk:

- *Invloed van spraakherkenning op gedrag deelnemers*
  Inzet van spraakherkenning kan een psychologisch effect hebben op het gedrag van de personen die deelnemen aan de vergadering of bijeenkomst. Het is bijvoorbeeld mogelijk dat men zich niet volledig durft uit te spreken en bepaalde zaken achterwege houdt omdat er een opname plaatsvindt met een integrale transcriptie.

- *Openbaarmaking transcripties*
  Wanneer tijdens vergaderingen spraakherkenning wordt ingezet, kan het zo zijn dat de opnames en transcripties van die vergaderingen vallen onder we Wet Open Overheid (Woo) en afhankelijk van de situatie in aanmerking komen voor openbaarheid. De Woo bepaalt namelijk dat iedereen het recht heeft op toegang tot publieke informatie zonder daartoe een belang te hoeven stellen, tenzij de wet anders bepaalt. Of dit recht op toegang ook geldt ten aanzien van door spraakherkenning voortgebrachte informatie zal per proces moeten worden

beoordeeld. Waar de Woo inderdaad van toepassing is, kan bovenstaand psychologisch effect versterkt worden.

4 Juridisch kader privacy en gegevensbescherming

In dit hoofdstuk analyseren wij het privacyrechtelijke kader dat van toepassing is op de ontwikkeling en toepassing van spraakherkenning. Allereerst staan we stil bij het grondwettelijke kader, vervolgens gaan we in op specifieke wetgeving die relevant is voor het JenV-domein: de AVG, de Wpg en de Wjsg. Welke van deze regimes van toepassing is, hangt af van het doel waarvoor persoonsgegevens worden verwerkt. Het gevolg hiervan is dat er mogelijk verschillende regimes van toepassing zijn op een reeks verwerkingen die achter of naast elkaar plaatsvinden.

4.1 Grondwettelijk kader

De artikelen 10-13 van de Grondwet regelen het recht op privacy in de breedste zin. Artikel 10 van de Grondwet bepaalt dat ieder behoudens bij of krachtens de wet te stellen beperkingen, recht heeft op eerbiediging van zijn persoonlijke levenssfeer. Diezelfde bepaling voegt daaraan toe dat de wet regels stelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. Een schending van het recht op privacy en gegevensbescherming is enkel toegestaan als dit in de wet in bepaald.

Ook op Europees niveau is het recht op privacy gegarandeerd als een fundamenteel recht. Dit komt onder meer tot uitdrukking in artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: 'EVRM'), waarin het recht op privacy als volgt wordt omschreven:

'1) Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2) Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn

van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten van anderen.'

Hoewel artikel 8 EVRM het recht op de bescherming van persoonsgegevens niet expliciet noemt, vormt het alsnog een onmisbaar onderdeel van het recht op respect voor privé- en gezinsleven, woning en correspondentie (met andere woorden: het recht op privacy) onder artikel 8 EVRM. In die zin wordt het recht op de bescherming van persoonsgegevens beschouwd als een modern en actief recht.[33]

Verder beschermt artikel 7 van het Handvest van de Grondrechten van de Europese Unie het recht op privacy. Artikel 8 van het Handvest regelt de bescherming van persoonsgegevens.

Het verdient tot slot opmerking dat het feit dat een JenV-organisatie (zoals de Rechtspraak en het OM) een grondwettelijk onafhankelijke status genieten, geen invloed heeft op de conclusies uit dit rapport voor wat betreft de juridisch verantwoorde inzet van spraakherkenning.

4.2 Algemene Verordening Gegevensbescherming (AVG)

4.2.1 Materiële en territoriale reikwijdte

De AVG is een Europese verordening die regels stelt voor de verwerking van persoonsgegevens. Onder 'verwerking' wordt op basis van artikel 4 sub 2 AVG verstaan:

'een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen,

[33] Zie voor verdere onderbouwing advocaat-generaal Sharpston die de zaak beschreef als twee afzonderlijke rechten: het "klassieke" recht op bescherming van de persoonlijke levenssfeer en een meer "modern" recht, de recht op gegevensbescherming, zie ook HvJ EU, gevoegde zaken C-92/09 en C-93/02, Volker und Markus Schecke GbR v. Land Hessen, conclusie van advocaat-generaal Sharpston, 17 juni 2010, punt 71.), een systeem van checks and balances invoeren om individuen te beschermen wanneer hun persoonsgegevens worden verwerkt. Zie ook Union européenne voor meer informatie. Agence des droits fondamentaux, de l'Europe, C., & Cour européenne des droits de l'homme. (2014). Handboek over de Europese wetgeving inzake gegevensbescherming. Publicatiebureau van de Europese Unie.

opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.'[34]

Onder een 'persoonsgegeven' wordt op basis van artikel 4 sub 1 AVG verstaan:

'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.'[35]

Spraak omvat informatie aan de hand waarvan – al dan niet in combinatie met andere persoonlijke attributen – een natuurlijk persoon geïdentificeerd kan worden (zie hierover ook hoofdstuk 2). Spraak kan daarom doorgaans als een persoonsgegeven worden gekwalificeerd. Om spraak om te zetten naar tekst vinden verschillende geautomatiseerde verwerkingen plaats, waaronder het verzamelen, vastleggen, ordenen, structureren, opslaan en gebruiken van persoonsgegevens (hier: spraak). Om deze redenen is de AVG in beginsel van toepassing op de verwerking van persoonsgegevens bij de toepassing van spraakherkenning (artikel 2 lid 1 AVG).

Voor bepaalde activiteiten waarbij persoonsgegevens worden verwerkt kan het zo zijn dat de AVG niet van toepassing is. Artikel 2 lid 2 sub d AVG regelt namelijk dat de AVG niet van toepassing is op de verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming

[34] Artikel 4(2) AVG
[35] Artikel 4(1) AVG.

tegen en de voorkoming van gevaren voor de openbare veiligheid. De verwerking van persoonsgegevens voor deze doeleinden wordt geregeld in de Wpg en de Wjsg.

Wat de territoriale reikwijdte betreft, is de AVG van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie al dan niet plaatsvindt (artikel 3 lid 1 AVG). Aangezien de verwerkingsverantwoordelijken binnen het JenV-domein in Nederland gevestigd zijn, is de AVG ook territoriaal gezien van toepassing op de toepassing van spraakherkenning door JenV en organisaties onder haar verantwoordelijkheid, tenzij die expliciet daarvan zijn uitgesloten, zoals in de vorige alinea genoemd.

4.2.2 Beginselen en grondslagen

De AVG bepaalt onder meer dat persoonsgegevens alleen mogen worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 5 lid 1 sub b AVG). Om vast te stellen of een verwerking van persoonsgegevens gerechtvaardigd is, moet het duidelijk zijn wat het doel van de verwerking is. De rechtvaardiging van de verwerking moet vervolgens gebaseerd worden op een van de grondslagen uit de AVG (zie artikel 6 lid 1 AVG). De grondslagen komen later in dit onderzoek aan bod.

Wanneer er een gerechtvaardigd doel is, mogen gegevens in beginsel verwerkt worden, indien aan de overige materiële eisen uit de AVG wordt voldaan. Het gaat dan om zaken als beveiliging, informatieplichten, transparantie en het invulling geven aan de rechten van de betrokkene(n).

Schematisch ziet de logica van de AVG er zo uit:

Afbeelding 5. Schematisch overzicht beginselen en grondslagen in de AVG.

Een verwerking is alleen toegestaan als deze gebaseerd kan worden op één van de grondslagen vermeld in artikel 6 lid 1 AVG. De grondslagen zijn niet cumulatief: het hebben van ten minste één grondslag is voldoende.

De zes mogelijke grondslagen zijn als volgt:

a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer

de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.[36]

Hierna bespreken we voor elk van deze grondslagen wanneer deze van toepassing is.

Toestemming (artikel 6 lid 1 sub a AVG

Onder toestemming van de betrokkene wordt verstaan: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt (artikel 4 lid 11 van de AVG).[37] Uit deze definitie blijkt dat een geldige toestemming aan een aantal vereisten moet voldoen:

1) Vrijelijk gegeven;
2) Specifiek;
3) Geïnformeerd; en
4) Ondubbelzinnig.

Vrijelijk gegeven:

Toestemming moet *vrij* gegeven zijn. Dat betekent dat het weigeren van de toestemming geen nadelige gevolgen voor de betrokkene mag hebben. Betrokkenen of hun wettelijk vertegenwoordigers mogen ook niet onder druk worden gezet om toestemming te geven. In gevallen waarin een ongelijke verhouding bestaat tussen de betrokkene en de verwerkingsverantwoordelijke, zal toestemming ook minder snel vrij gegeven kunnen worden.

Dit vereiste houdt in dat er een reële keuze en controle is voor de betrokkenen. Indien de betrokkene geen echte keuze heeft, zich gedwongen voelt om zijn toestemming te geven,

[36] De grondslag onder f geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken en zal om die reden in dit rapport grotendeels buiten beschouwing blijven.
[37] Kinderen vanaf 16 jaar kunnen zelf toestemming geven. Voor de verwerking van persoonsgegevens betreffende kinderen onder de 16 op basis van de grondslag toestemming, is de toestemming van de wettelijk vertegenwoordigers vereist (artikel 5 lid 1 Uitvoeringswet AVG).

of negatieve gevolgen ondervindt indien hij zijn toestemming niet geeft, is die toestemming niet geldig. De betrokkene mag dus geen negatief gevolg ondervinden indien toestemming niet wordt gegeven. Dit is bepaald in overweging 42 van de AVG die voorschrijft dat de verwerkingsverantwoordelijke moeten kunnen aantonen dat een betrokkene zijn toestemming kan weigeren of intrekken zonder daarvan nadeel te ondervinden. Daarnaast wordt in overweging 43 van de AVG uitgelegd dat toestemming nooit vrijelijk gegeven kan worden wanneer er een scheve machtsverhouding bestaat tussen de betrokkene en de verwerkingsverantwoordelijke, met name wanneer die partij een overheidsinstantie is.

Van een scheve verhouding is bijvoorbeeld vaak sprake in het kader van de arbeidsverhouding.[38] Vanwege de afhankelijkheid die voortvloeit uit de relatie tussen werkgever en werknemer, is het niet waarschijnlijk dat een betrokkene zijn werkgever toestemming voor de gegevensverwerking kan weigeren zonder dat hieraan negatieve gevolgen zijn verbonden. Dit betekent niet dat werkgevers zich nooit kunnen beroepen op toestemming als rechtsgrond voor de verwerking. Er kunnen zich situaties voordoen waarin een werkgever persoonsgegevens van een werknemer mag verwerken op basis van toestemming. De werknemer moet een keuze hebben en er mag geen sprake zijn van bedrog, intimidatie of dwang. Ook mag de betrokkene geen negatieve gevolgen riskeren wanneer hij niet toestemt.

Specifiek:

De toestemming moet worden gegeven voor een duidelijk en afgebakend verwerkingsdoel. Dit betekent ook dat wanneer er sprake is van meerdere verwerkingsdoelen. De toestemming wordt geacht niet vrijelijk te zijn verleend indien geen afzonderlijke toestemming kan worden gegeven voor verschillende verwerkingen daar waar dit wel passend is.

Geïnformeerd:

[38] Artikel 88 en overweging 155 AVG.

Dit houdt in dat een verwerkingsverantwoordelijke bepaalde informatie aan de betrokkene moet verstrekken voordat deze toestemming geeft. Overeenkomstig overweging 42 van de AVG moet de betrokkene ten minste op de hoogte zijn van: i) de identiteit van de voor de verwerking verantwoordelijke, en ii) de doeleinden van de verwerking waarvoor de persoonsgegevens zijn bestemd. In het algemeen vereist geïnformeerde toestemming dat de verwerkingsverantwoordelijke de betrokkene duidelijk uitlegt waarmee hij instemt, in een taal die voor de betrokkene begrijpelijk is.

Ondubbelzinnig:

Toestemming onder de AVG moet worden gegeven door middel van een duidelijke ondubbelzinnige indicatie van de wensen van de betrokkene waarmee hij of zij, door een verklaring of door een duidelijke bevestigende handeling, instemt met de verwerking van persoonsgegevens. Het moet duidelijk zijn dat de betrokkene zijn toestemming heeft gegeven. Indien er enige twijfel bestaat, is de toestemming niet geldig.

Herroepbaar:

Artikel 7, lid 3, AVG bepaalt dat toestemming alleen geldig is als zij ook kan worden herroepen. Dit houdt in dat de betrokkene het recht moet hebben zijn toestemming te allen tijde in te trekken.

Kwetsbare groepen

Voor bepaalde kwetsbare doelgroepen stelt de AVG bovendien zwaardere eisen aan het verlenen van toestemming voor de verwerking van persoonsgegevens. Zo stelt artikel 8 AVG bijvoorbeeld specifieke voorwaarden voor de toestemming van kinderen. Meer in het bijzonder stelt deze bepaling dat indien diensten van de informatiemaatschappij direct worden aangeboden aan een kind, de verwerking van persoonsgegevens van een kind in principe rechtmatig is wanneer het kind ten minste 16 jaar oud is. Voor kinderen die jonger zijn dan 16 jaar oud geldt dat een dergelijke verwerking enkel rechtmatig is indien en voor

zover de toestemming of machtiging in dit verband wordt verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt. Let wel, het voorgaande geldt enkel indien de toestemming van het kind als grondslag voor de verwerking van persoonsgegevens wordt ingezet.

Uitvoering van een overeenkomst (artikel 6 lid 1 sub b AVG

Persoonsgegevens mogen worden verwerkt wanneer dit noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen. Het moet hierbij gaan om een overeenkomst met de betrokkene zelf (bijvoorbeeld een arbeidsovereenkomst). Voor de gegevensuitwisselingen die in dit rapport aan de orde komen, zal deze grondslag waarschijnlijk niet snel van toepassing zijn omdat de betrokkenen geen overeenkomst met JenV hebben.[39]

Wettelijke plicht (artikel 6 lid 1 sub c AVG)

Wanneer er een wettelijke plicht bestaat tot het delen van gegevens, dan kan artikel 6 lid 1 sub c AVG als grondslag dienen. Deze plicht moet wel concreet zijn: bijvoorbeeld het voldoen aan een vordering tot verstrekking van bepaalde persoonsgegevens door de politie, of de verplichting op grond van de belastingwetgeving om een loonadministratie te voeren. Een algemene taakstelling voor een overheidsinstantie, levert nog geen wettelijke plicht op om persoonsgegevens te verwerken. Wel kan het noodzakelijk zijn dat, teneinde die taak uit te voeren, persoonsgegevens verwerkt moeten worden. In dat geval zal de grondslag niet de wettelijke plicht zijn, maar veeleer de taak van algemeen belang of de uitoefening van openbaar gezag (zie hiervoor de nadere uitleg hieronder over artikel 6 lid 1 sub e AVG).

Vitale belangen (artikel 6 lid 1 sub d AVG)

[39] Een mogelijke uitzondering is de arbeidsovereenkomst, wanneer het gaat om het gebruik van spraakherkenning door medewerkers. Het is dan wel de vraag in hoeverre de verwerking noodzakelijk is voor de goede uitvoer van de arbeidsovereenkomst.

Persoonsgegevens mogen worden verstrekt wanneer dit noodzakelijk is om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen. Deze grondslag ziet op situaties waarin de betrokkene (degene wiens persoonsgegevens worden verstrekt) of een andere natuurlijke persoon in een levensbedreigende situatie verkeert en niet in staat is om toestemming te geven. Bijvoorbeeld in het geval van acuut gevaar voor het leven of een potentieel levensbedreigende situatie. Gebruik van deze grondslag is in beginsel alleen mogelijk als de verwerking kennelijk (dat wil zeggen: duidelijk) niet op een andere grondslag gebaseerd kan worden, bijvoorbeeld toestemming of een taak van algemeen belang/openbaar gezag.[40]

Taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag (artikel 6 lid 1 sub e AVG)

In het kader van dit rapport biedt met name artikel 6 lid 1 sub e AVG een passende grondslag voor de toepassing van spraakherkenning. Wanneer de verwerking van persoonsgegevens wordt verricht op basis van deze grondslag dient, net zoals dat voor de wettelijke plicht onder artikel 6 lid 1 sub c geldt, de verwerking een grondslag te hebben in het Unierecht of het lidstatelijke recht (overweging 45 AVG). De AVG schrijft niet voor dat voor elke afzonderlijke verwerking specifieke wetgeving vereist is; er kan worden volstaan met wetgeving die als basis fungeert voor verscheidene verwerkingen die zich op deze grondslag baseren. Ook dient dergelijke wetgeving te bepalen wat het doel van de verwerking is en wie belast is met het uitvoeren van een taak van algemeen belang dan wel met een taak in het kader van de uitoefening van openbaar gezag.

Gerechtvaardigd belang (artikel 6 lid 1 sub f AVG)

Indien gegevens verstrekt worden op basis van een gerechtvaardigd belang, dient aan de volgende drie voorwaarden te zijn voldaan:

1. *Gerechtvaardigd*

[40] Verordening (EU) 2016/679 (Algemene Verordening Gegevensbescherming), overweging 46.

Allereerst moet de verwerkingsverantwoordelijke een belang nastreven dat 'gerechtvaardigd' is. In de meest recente rechtspraak is hierover bepaald dat de verwerkingsverantwoordelijke geen belang mag nastreven dat in strijd is met de wet.[41]

2. *Noodzakelijkheid*

   Hier dient allereerst de proportionaliteit van de verstrekking van persoonsgegevens beoordeeld te worden: staat de verstrekking van persoonsgegevens in verhouding tot het doel van de verstrekking. Daarnaast dient ook de subsidiariteit van de verstrekking te worden beoordeeld. Met andere woorden er moet geen minder ingrijpend middel voorhanden zijn.

3. Afweging belangen

   Ten slotte wordt het belang van de verwerkingsverantwoordelijke gewogen tegen dat van de betrokkene aan de hand van de volgende criteria:

   - de gevolgen voor de betrokkene;
   - de (aanvullende) waarborgen die de verwerkingsverantwoordelijke of derde heeft getroffen om ongewenste gevolgen voor de betrokkene te voorkomen of beperken;
   - de ernst van de inmenging op het grondrecht van de betrokkene;
   - of de betrokkene de verwerking redelijkerwijs kan verwachten, bijvoorbeeld als vervolg op een eerdere verwerking waarvoor diegene toestemming heeft gegeven of als vervolg op verwerkingen die noodzakelijk zijn om een contract uit te voeren.

Blijken de belangen van de betrokkene zwaarder te wegen? Dan mag de verwerking niet plaatsvinden op basis van de grondslag gerechtvaardigd belang. Wegen de belangen van de verwerkingsverantwoordelijke of derde zwaarder? Dan heeft de verwerkingsverantwoordelijke een grondslag om de persoonsgegevens te verwerken.

[41] Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111.

Belangrijk om op te merken is dat de grondslag 'gerechtvaardigd belang' niet geldt voor een verwerking van persoonsgegevens door overheidsinstanties in het kader van de uitoefening van hun taken. De ratio hierachter is dat de taken van de overheid, en in het verlengde daarvan de reikwijdte van hun mogelijkheden voor verwerking van persoonsgegevens, in wetgeving vervat moeten zijn.

De grondslag gerechtvaardigd belang kan wel door de overheid worden ingezet voor facilitaire doeleinden. Wanneer bijvoorbeeld spraakherkenning wordt gebruikt om op een meer efficiëntie wijze de bedrijfsmiddelen in te zetten, dan zou 6f AVG de geëigende grondslag zijn. Het hangt er dan uiteraard wel vanaf of de verwerking noodzakelijk is en de belangen van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkenen.

Voor alle grondslagen geldt: noodzakelijkheid.

Voor alle hierboven genoemde grondslagen is een belangrijk vereiste dat de verwerking noodzakelijk is om het beoogde doel te bereiken. Om noodzakelijk te zijn moet de verstrekking allereerst in verhouding staan tot het beoogde doel (proportionaliteit). In essentie houdt dit in dat niet meer persoonsgegevens mogen worden verwerkt dan noodzakelijk voor het beoogde doel. Daarnaast mogen er ook geen minder ingrijpende alternatieven voor handen zijn (subsidiariteit). Wil een verwerkingsverantwoordelijke persoonsgegevens verwerken, dan moet deze dus de noodzakelijkheid van de verwerking kunnen aantonen.

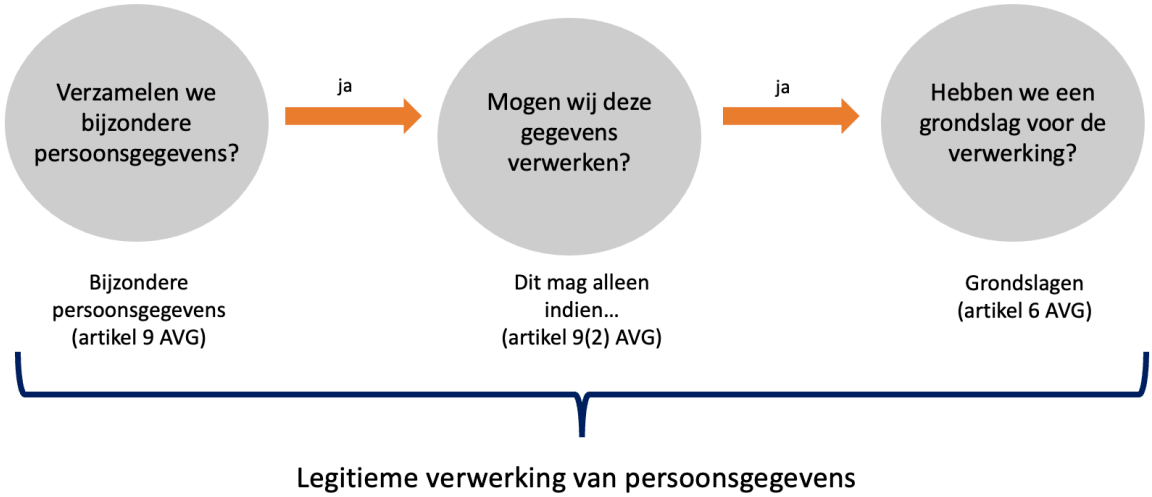
Of een verwerking noodzakelijk is, moet van geval tot geval beoordeeld worden op basis van de relevante omstandigheden. Dit hangt mede af van de hoeveelheid en het soort persoonsgegevens dat wordt verwerkt en het doel van de verwerking.

4.2.3 Bijzondere persoonsgegevens

Naast 'gewone' of 'algemene' persoonsgegevens, zoals naam, adres of woonplaats, kent de AVG ook bijzondere categorieën persoonsgegevens (hierna: 'bijzondere

persoonsgegevens'). Bijzondere persoonsgegevens zijn persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Een verwerking van bijzondere persoonsgegevens is in beginsel verboden (artikel 9 lid 1 AVG), tenzij er een uitzondering van toepassing is. Om die reden moet de verwerking, naast een van de rechtsgronden in artikel 6 AVG, ook voldoen aan een van de uitzonderingsgronden voor de verwerking van bijzondere persoonsgegevens in artikel 9 AVG. In onderstaande afbeelding wordt deze logica gevisualiseerd:



Afbeelding 6. Overzicht voorwaarden legitieme verwerking bijzondere persoonsgegevens.

Ten aanzien van de verwerking van persoonsgegevens ten behoeve van de training en toepassing van spraakherkenning in meer algemene zin heeft de EDPB in de *EDPB Guidelines on Virtual Voice Assistants* het volgende benadrukt: *"The EDPB recalls that voice data is inherrently biometric personal data."*[42] In lijn met deze redenering kan in het kader

[42] EDPB (2021). Guidelines 02/2021 on virtual voice assistants . Version 2.0. Geraadpleegd op 16 september 2022, van https://edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf.

van de training en toepassing van spraakherkenning worden uitgegaan van een verwerking van biometrische gegevens wanneer spraak wordt omgezet naar tekst.

Of spraak naast een biometrisch persoonsgegeven ook een bijzonder persoonsgegeven is, hangt af van of hiermee de unieke identificatie van een persoon wordt beoogd.[43] In de EDPB *Guidelines 3/2019 on processing of personal data through video devices* heeft de EDPB ten aanzien van de kwalificering van biometrische gegevens als bijzondere persoonsgegevens het belang van deze unieke identificatie benadrukt. De EDPB onderstreept in deze richtsnoeren dat videobeelden van een persoon op zichzelf niet kunnen worden beschouwd als biometrische gegevens in de zin van artikel 9 AVG, als deze niet specifiek zijn verwerkt om bij te dragen aan de identificatie van een persoon.[44] Waar het een verwerking van een biometrisch gegeven betreft bij de toepassing van spraakherkenning, kan een vergelijkebare redenering worden gehanteerd. Aangezien spraakherkenning niet de unieke identificatie van personen tot doel heeft, kwalificeert spraak in de context van spraakherkenning in principe niet als een bijzonder persoonsgegeven.[45]

Kwalificatie van spraak als biometrisch of bijzonder persoonsgegeven

Wanneer spraak automatisch wordt omgezet in tekst is er sprake van een verwerking van een biometrisch persoonsgegeven. Een biometrisch persoonsgegeven is pas een bijzonder persoonsgegeven wanneer dit gegeven wordt gebruikt om een persoon te identificeren. Dit betekent dat wanneer JenV een audiofragment opneemt om dit automatisch om te zetten in tekst in beginsel geen sprake is van een verwerking van een bijzonder persoonsgegeven. Wanneer spraak wordt gebruikt om personen te identificeren, wordt spraak aangemerkt als biometrisch persoonsgegeven dat tevens kwalificeert als een bijzonder persoonsgegeven.

[43] Artikel 9 lid 1 AVG spreekt van 'biometric data for the purpose of uniquely identifying an individual'
[44] EDPB (2020). Guidelines 3/2019 on processing personal data through video devices. Version 2.0. Geraadpleegd op 16 september 2022, van https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf, p. 18.
[45] Zie in dit kader ook de redenering van de Autoriteit Persoonsgegevens inzake camerabeelden en bijzondere persoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf.

Naast spraak op zich, kunnen ook de inhoudelijke elementen van spraak gevoelige informatie over een persoon bevatten (denk bijvoorbeeld aan gesprekken over politiek of identiteit). Bovendien geldt dat, afhankelijk van capaciteiten van de spraakherkenningstechnologie, bepaalde assumpties over de emotionele en fysieke gezondheid van de betrokkene gemaakt kunnen worden. Strikt genomen kwalificeren deze gegevens op zichzelf onder de AVG als bijzondere persoonsgegevens. In het kader van de opname van beeldmateriaal, nuanceerde de Autoriteit persoonsgegeven (hierna: 'AP') in 2016 in haar beleidsregels cameratoezicht dat aspecten als gezondheid, geloofsovertuiging en ras uit beeldmateriaal kunnen worden afgeleid maar dat daarmee het cameratoezicht – en dus de verwerking van deze persoonsgegevens - zelf nog niet onaanvaardbaar is. De reden hiervoor is dat de AP camerabeelden van een persoon niet als bijzondere persoonsgegevens beschouwt als de verwerking van voornoemde bijzondere persoonsgegevens (als 'bijvangst') onvermijdelijk is, het doel niet is gericht op het daadwerkelijk onderscheid maken op basis van die bijzondere persoonsgegevens en verondersteld mag worden dat dit ook niet zal gebeuren. Deze redenering ten aanzien van de kwalificering van bijzondere persoonsgegevens is later door de Hoge Raad bevestigd[46] en ook de EDPB gaat mee in deze redenering. In aanvulling op overweging 51 AVG[47] stelt zij in haar *Guidelines 3/2019 on processing of personal data through video devices* dat videobewaking niet altijd als de verwerking van bijzondere persoonsgegevens kan worden beschouwd; slechts wanneer videobeelden worden verwerkt om bijzondere persoonsgegevens af te leiden, is artikel 9 AVG van toepassing.[48] Wanneer deze argumentatie wordt toegepast op de verwerkingsactiviteiten ten gevolge van de toepassing van spraakherkenning, geldt eveneens dat bij de beantwoording van de vraag of bij de toepassing van spraakherkenning al dan niet sprake is van de verwerking van bijzonder persoonsgegevens in de zin van artikel 9 AVG rekening dient te worden gehouden met het doel en de context van de verwerking. Gezien de werking van en

[46] HR 27 juni 2017, ECLI:NL:HR:2017:1166.
[47] Overweging 51 AVG stelt dat de verwerking van foto's niet systematisch mag worden beschouwd als de verwerking van bijzondere categorieën persoonsgegevens.
[48] EDPB (2020). Guidelines 3/2019 on processing personal data through video devices. Version 2.0. Geraadpleegd op 16 september 2022, van https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf, p. 17.

doeleinden waartoe spraakherkenning wordt ingezet, zal naar ons oordeel in principe geen sprake zijn van de verwerking van bijzondere persoonsgegevens in de zin van artikel 9 AVG.

Hoewel spraak dus niet persé een bijzonder persoonsgegeven is, moet wel rekening worden gehouden met het gevoelige karakter van deze gegevens. De gevoeligheid van de gegevens speelt allereerst een rol in de beoordeling van de proportionaliteit van een verwerking. Daarnaast moet bij het treffen van technische en organisatorische maatregelen rekening worden gehouden met de gevoeligheid van de gegevens.[49]

4.2.4 Gegevens van strafrechtelijke aard

Naast bijzondere persoonsgegevens, kent de AVG gegevens over *"strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen"*, oftewel: gegevens van strafrechtelijke aard.

Hieronder worden gegevens verstaan die betrekking hebben op een veroordeling, maar ook op min of meer gegronde verdenkingen.[50] Het moet gaan om zodanig concrete feiten en omstandigheden dat zij een bewezenverklaring in de zin van art. 350 Sv kunnen dragen.[51] Artikel 1 UAVG bepaalt dat onder de definitie van persoonsgegevens van strafrechtelijke aard ook persoonsgegevens vallen die betrekking hebben op een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag. Het moet dan wel gaan om een maatregel met een punitief karakter.[52]

Strafrechtelijke gegevens mogen alleen worden verwerkt onder toezicht van de overheid of wanneer de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden (artikel 10 AVG).

[49] EDPB (2020). Guidelines 3/2019 on processing personal data through video devices. Version 2.0. Geraadpleegd op 16 september 2022, van https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf, p. 17.
[50] De Vries, in: T&C Algemene Verordening Gegevensbescherming (AVG) inclusief Uitvoeringswet AVG, art. 31 UAVG, aantekening, p. 341.
[51] HR 29 mei 2009, ECLI:NL:HR:2009:BH4720.
[52] ECLI:NL:GHDHA:2019:3539.

Deze lidstaatrechtelijke bepalingen zijn onder meer te vinden in de UAVG. Artikel 31 UAVG bepaalt dat verwerking van strafrechtelijke gegevens slechts is toegestaan in de gevallen genoemd in artikelen 32 en 33 UAVG. Zo mogen persoonsgegevens van strafrechtelijke aard onder meer verwerkt worden indien de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden (artikel 32 sub a UAVG). Zoals reeds opgemerkt in paragrafen 4.1.2.2 en 4.1.2.3 moet deze toestemming in vrijheid zijn gegeven, hetgeen vaak problematisch is in de verhouding tussen burger en overheid.

Verder mogen persoonsgegevens van strafrechtelijke aard op grond van de AVG en de UAVG verwerkt worden indien de verwerking geschiedt door organen die krachtens de wet zijn belast met de toepassing van het strafrecht, zoals bijvoorbeeld geldt voor de Reclassering. Daarnaast mogen verwerkingsverantwoordelijken persoonsgegevens van strafrechtelijke aard verwerken indien zij deze hebben verkregen krachtens de Wpg of de Wjsg (artikel 33 lid 1 sub a UAVG). De precieze rol en betekenis van de Wpg en de Wjsg in de context van spraakherkenning komen aan bod in 4.1.3 en 4.1.4.

Indien voldaan is aan een van de uitzonderingsgronden uit artikel 32 of 33 UAVG, betekent dit niet dat daarmee de verwerking van strafrechtelijke gegevens zonder meer is toegestaan. Er moet naast een uitzonderingsgrond ook altijd een grondslag uit artikel 6 AVG van toepassing zijn. Onderstaande afbeelding visualiseert deze logica.

Afbeelding 7. Overzicht voorwaarden legitieme verwerking strafrechtelijke gegevens.

4.2.5 Geautomatiseerde besluitvorming

De AVG omvat een aantal rechten van betrokkenen ten aanzien van de verwerking van persoonsgegevens, waaronder ook in het kader van geautomatiseerde individuele besluitvorming. Meer in het bijzonder bepaalt artikel 22 AVG dat een betrokkene het recht heeft om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.

Dezelfde bepaling stelt dat dit verbod niet geldt voor zover een dergelijk besluit noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke, Unierechtelijke of lidstaatrechtelijke bepalingen die op een verwerkingsverantwoordelijke van toepassing zijn en die ook voorzien in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene, of indien een dergelijk besluit berust op de uitdrukkelijke toestemming van de betrokkene. Bovendien bepaalt het vierde lid van deze bepaling dat automatische besluitvorming op basis van de in het tweede lid genoemde uitzonderingen niet gebaseerd kunnen worden op bijzondere categorieën persoonsgegevens ex artikel 9 AVG (zie hiervoor 4.2.3), tenzij de voorwaarden uit lid 2 sub a (uitdrukkelijke toestemming) of g (noodzakelijk om redenen van zwaarwegend algemeen

belang) van die bepaling van toepassing zijn én er passende maatregelen ter bescherming van de gerechtvaardigde belangen van de betrokkene zijn getroffen.

Wat betreft de eerst en laatstgenoemde gevallen dient de verwerkingsverantwoordelijke passende maatregelen te treffen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene, waaronder ten minste het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke, het recht om zijn om haar standpunt kenbaar te maken en het recht om het besluit in kwestie aan de vechten. Wat betreft de eerste maatregel – menselijke tussenkomst – is het relevant een onderscheid te maken tussen de verschillende manieren waarop binnen de werking van AI de interactie tussen mens en machine bepaald is. In dit kader kan onderscheid gemaakt worden tussen AI die uitgaat van een:

1) *human-in-the-loop* benadering (de benadering waarbij de mens centraal staat in de ontwikkeling en toepassing van/besluitvorming door AI);
2) een *human-out-of-the-loop* benadering (de benadering waarbij de mens op de achtergrond wordt geplaatst in de ontwikkeling en toepassing van/besluitvorming door AI); en
3) een *human-over-the-loop* bandering (i.e. de benadering waarbij de mens in staat wordt gesteld tijdens het AI-gedreven besluitvormingsproces parameters aan te passen).

Met betrekking tot spraakherkenning rijst de vraag in hoeverre er sprake is van automatische besluitvorming. Deze vraag wordt in dit rapport later besproken.

4.3 Wet Politiegegevens en Wet Justitiële gegevens

4.3.1 Richtlijn politie- en justitiegegevens

De bescherming van persoonsgegevens is een grondrecht dat in het Handvest van de grondrechten van de Europese Unie is vastgelegd. Om de privacy van burgers te waarborgen en te zorgen voor een effectieve rechtspleging in Europa is de Richtlijn politie- en justitiegegevens aangenomen.[53]

[53] Richtlijn 2016/680/EG (Richtlijn politie- en justitiegegevens).

Deze Richtlijn kent een tweeledig doel:

1) Het beschermen van de grondrechten en de fundamentele vrijheden van natuurlijke personen, in het bijzonder de bescherming van hun persoonsgegevens.
2) Erop toe te zien dat de legitieme uitwisseling van persoonsgegevens door bevoegde autoriteiten binnen de EU niet wordt beperkt of verboden om redenen die verband houden met de bescherming van persoonsgegevens.

Om deze doelen te bereiken regelt de Richtlijn de zorgvuldige verwerking van politie- en justitie gegevens door de bevoegde autoriteiten bij de voorkoming, opsporing en vervolging van strafbare feiten en de tenuitvoerlegging van straffen en maatregelen. De Richtlijn beoogt de waarborgen bij de verwerking van hun persoonsgegevens op een gelijkwaardig hoog niveau te brengen en de uitwisseling van persoonsgegevens tussen de lidstaten te vergemakkelijken.

De Richtlijn en de AVG vormen een samenhangend pakket van maatregelen ter bescherming van de persoonlijke levenssfeer binnen de Europese Unie. De AVG is van toepassing op (nagenoeg) alle verwerkingen van persoonsgegevens, maar de verwerkingen van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, opsporing en vervolging van strafbare feiten en de tenuitvoerlegging van straffen en maatregelen zijn expliciet uitgezonderd van het toepassingsbereik van de AVG. Op deze verwerkingen is de Richtlijn van toepassing.

De Richtlijn is, anders dan de AVG, niet rechtstreeks van toepassing in de lidstaten van de Europese Unie. De bepalingen uit een Richtlijn dienen geïmplementeerd te worden in nationale wetgeving alvorens zij werking treffen. In Nederland is dat gedaan in de Wet Politiegegevens (Wpg) en de Wet Justitiële gegevens (Wjsg) alsmede de daarbij behorende besluiten en regelingen. Hier wordt in onderstaande paragrafen nader op ingegaan.

4.3.2 Wet Politiegegevens (Wpg)

De politie is belast met de handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. De politie voert de handhavingstaak uit onder gezag van de Officier van Justitie en de hulpverleningstaak en de openbare orde-taak onder het gezag van de burgemeester. Om haar politietaak goed uit te kunnen voeren, verwerkt de politie persoonsgegevens.

Een politiegegeven wordt in de Wpg gedefinieerd als: "*elk persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt*."

De politietaak is in de Politiewet 2012 als volgt beschreven: *"De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met* de *geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven."*

Omdat dit in beginsel een inbreuk op de persoonlijke levenssfeer van de betrokkene omvat, heeft de politie hiervoor een wettelijke basis nodig.[54] De wettelijke basis voor het verwerken van politiegegevens is vastgelegd in de Wpg. Met het oog op de relevantie voor dit onderzoek, zal in het navolgende worden stilgestaan bij de juridische voorwaarden voor het verwerken van politiegegevens.

4.3.2.1 Rechtmatige verwerking van politiegegevens

Politiegegevens mogen uitsluitend worden verwerkt voor bij de wet vastgestelde doelen, met andere woorden, voor de politietaak. De verwerking van politiegegevens met het oog op de uitvoering van de politietaak omvat op grond van de Wpg de volgende situaties:

- De uitvoering van de dagelijkste politietaak (artikel 8 Wpg);
- Gerichte verwerking van politiegegevens (artikel 9 en 10 Wpg);
- Het geautomatiseerd vergelijken en in combinatie doorzoeken van gegevens (artikel 11 Wpg);

[54] EHRM, 6 juni 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. no. 62332/00.

- Ten behoeve van de controle op en het beheer van informanten (artikel 12 Wpg); en
- Ten behoeve van ondersteunende taken (artikel 13 Wpg).

Daarnaast bepaalt de Wpg in artikel 5 ten aanzien van bijzondere categorieën politiegegevens, dat deze enkel mogen worden verwerkt voor zover dit onvermijdelijk is voor het doel van de verwerking, in aanvulling op de verwerking van andere politiegegevens betreffende de persoon en de gegevens afdoende zijn beveiligd. Zoals in paragraaf 4.2.3. is uitgelegd, kwalificeert spraak als een biometrisch persoonsgegeven. Of spraak naast een biometrisch persoonsgegeven ook een bijzonder persoonsgegeven is, hangt af van of hiermee de unieke identificatie van een persoon wordt beoogd.[55]

4.3.2.2 Het ter beschikking stellen van politiegegevens

Met het ter beschikking stellen van politiegegevens wordt bedoeld: het verstrekken van politiegegevens aan personen (binnen het Wpg-domein) die overeenkomstig de wet zijn geautoriseerd voor het verwerken van politiegegevens.[56] Onder het Wpg-domein vallen de politie, Koninklijke Mareschaussee, Rijksrecherche, en bijzondere opsporingsambtenaren.

Politiegegevens worden binnen het Wpg-domein ter beschikking gesteld indien dit noodzakelijk is voor de uitvoering van een politietaak. Politiegegevens mogen enkel ter beschikking worden gesteld aan personen die geautoriseerd zijn om die politiegegevens te verwerken. Wanneer politiegegevens worden verstrekt aan een politieambtenaar voor een ander doel dan de uitvoering van een politietaak, dan kan niet van een 'ter beschikkingstelling van politiegegevens' worden gesproken. In dit geval is er sprake van 'verstrekking', waarvoor een ander regime geldt (zie onder).

Politiegegevens moeten ter beschikking worden gesteld aan:

[55] Artikel 9 lid 1 AVG spreekt van 'biometric data for the purpose of uniquely identifying an individual'
[56] Artikel 1 sub e Wpg.

- Geautoriseerde politieambtenaren wanneer deze gegevens noodzakelijk zijn voor de uitvoering van de politietaak waarvoor de politieambtenaar geautoriseerd is.
- Geautoriseerde personen die geen politieambtenaar zijn indien het noodzakelijk is voor de uitvoering van de politietaak. In uitzonderingsgevallen kunnen personen die geen ambtenaar van de politie zijn, worden geautoriseerd om politiegegevens te verwerken.
- Bevoegde autoriteiten, organen of instanties die met een politietaak belast zijn kunnen politiegegevens van een andere lidstaat ontvangen, indien dit volgt uit een rechtsinstrument. In de Wpg en het bijbehorende Besluit politiegegevens (hierna: 'Bpg') staan nadere voorwaarden omschreven over gegevensdeling met andere landen.

Naast de hierboven omschreven algemene bepalingen omtrent terbeschikkingstelling (art. 15 Wpg) zijn in de artikelen 8, 9, 10, 12 en 13 Wpg nadere voorwaarden opgenomen voor de ter beschikkingstelling van politiegegevens.

4.3.2.3 Het verstrekken van politiegegevens

Met het verstrekken van politiegegevens wordt bedoeld: het bekend maken of ter beschikking stellen van politiegegevens.[57] De Wpg kent in beginsel een 'gesloten verstrekkingsregime'. Dit houdt in dat Politiegegevens uitsluitend verstrekt mogen worden indien dit noodzakelijk is en alleen aan personen en/of organisaties die zijn opgenomen in de Wpg en het Bpg en onder de voorwaarden die worden genoemd in de Wpg en het Bpg.

De volgende verstrekkingsmogelijkheden zijn opgenomen in de Wpg:

- Verstrekkingen aan gezagsdragers en opsporingsambtenaren (artikel 16 Wpg);
- Verstrekkingen aan inlichtingendiensten (artikel 17 Wpg);
- Verstrekkingen aan derden structureel (artikel 18 Wpg);
- Verstrekkingen aan derden incidenteel (artikel 19 Wpg);

[57] Artikel 1 sub d Wpg.

- Verstrekkingen aan derden structureel voor samenwerkingsverbanden (artikel 20 Wpg);
- Verstrekkingen aan derden ten behoeve van wetenschappelijk onderzoek en statistiek (artikel 22 Wpg); en
- Rechtstreekse verstrekkingen (artikel 23 en 24 Wpg).

4.3.3 Wet Justitiële en Strafvorderlijke gegevens (Wjsg)

De regels voor het verzamelen en verder verwerken van persoonsgegevens door organisaties die vallen onder JenV voor het uitvoeren van strafrechtelijke beslissingen en gegevens betreffende rechtspersonen met het oog hierop is vastgelegd in de Wet justitiële en strafvorderlijke gegevens ('Wjsg').

De Wjsg is van toepassing op het verwerken van (i) justitiële gegevens, (ii) strafvorderlijke gegevens, (iii) persoonsdossiers, (iv) tenuitvoerleggingsgegevens en (v) gerechtelijke strafgegevens (hierna tezamen aangeduid als: 'Wjsg-gegevens'). Voor elk van deze categorieën geeft de Wjsg een aparte regeling.

Justitiële gegevens worden in de Wjsg als volgt omschreven: 'bij algemene maatregel van bestuur te omschrijven gegevens inzake de toepassing van het strafrecht of de strafvordering die in een gegevensbestand zijn of worden verwerkt. In het Besluit Justitiële en Strafvorderlijke gegevens (hierna: 'Bjsg') is vervolgens opgenomen welke gegevens worden aangemerkt als justitiële gegevens. Als justitiële gegevens worden onder meer aangemerkt de gegevens op basis waarvan het mogelijk is een persoon of organisatie te identificeren, zoals naam, adres, geboortedatum en persoonsidentificerende nummers en gegevens die betrekking hebben op het (mogelijke) strafbare feit dat is gepleegd, zoals beslissingen van het OM, de rechter, de strafbepaling en datum waarop (of periode waarin) zich een strafbaar feit heeft voorgedaan.

Strafvorderlijke gegevens zijn gegevens die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het OM in een strafdossier of langs geautomatiseerde weg

in een bestand verwerkt. Hieronder vallen niet alleen de processen-verbaal van de politie, maar ook beslissingen die de officier van justitie of de rechter-commissaris heeft genomen in het kader van een strafvorderlijk onderzoek.

Ook *persoonsdossiers* vallen onder de reikwijdte van de Wjsg. Met een persoonsdossier wordt bedoeld een gestructureerd dossier waarin de aan de rechtelijke autoriteiten uitgebrachte rapporten over onderzoeken naar het gedrag of de levensomstandigheden van een natuurlijk persoon in verband met tegen hem aanhangige strafzaken, de tenuitvoerlegging van aan hem opgelegde straffen of maatregelen of zijn reclassering, zijn opgenomen.

Tenuitvoerleggingsgegevens betreffen gegevens die betrekking hebben op de tenuitvoerlegging van straffen en maatregelen. In tegenstelling tot bij de opsporing is bij de tenuitvoerlegging de afdoening al bekend. Onder het begrip tenuitvoerleggingsgegevens vallen ook de verwerking van persoonsgegevens ter uitvoering van de Penitentiaire beginselenwet, de Beginselenwet Justitiële Jeugdinrichtingen en de Beginselenwet verpleging ter beschikking gestelden. Ook de gegevens die betrekking hebben op de uitvoering van een strafbeschikking worden aangemerkt als tenuitvoerleggingsgegevens. Voor de Wet administratiefrechtelijke handhaving verkeersvoorschriften geldt dat het afhangt van de aard van de beslissing of de Wjsg daarop ook van toepassing is. In beginsel is de Wjsg van toepassing op het moment dat de beslissing een strafrechtelijke afdoening inhoudt. Indien gelet op de aard en ernst van de overtreding een administratiefrechtelijke beslissing is getroffen, zoals bij enkele snelheidsovertredingen het geval kan zijn, is op de tenuitvoerlegging daarvan de AVG en UAVG van toepassing en niet de Wjsg.

Gerechtelijke strafgegevens zijn gegevens die worden verwerkt door de gerechtelijke instanties in het kader van de behandeling van strafzaken. Hier moet worden gedacht aan alle gegevens die worden verwerkt door gerechten op strafrechtelijk gebied bij de uitvoering van gerechtelijke taken. Expliciet wordt nog benoemd dat hieronder niet de

gegevens vallen die in het kader van burgerlijke of bestuursrechtelijke zaken worden verwerkt door gerechtelijke instanties. De persoonsgegevens die in het kader daarvan worden verwerkt, vallen binnen de reikwijdte van de Algemene Verordening Gegevensbescherming.

4.3.3.1 Rechtmatige verwerking van Wjsg-gegevens

In de Wjsg is uitdrukkelijk aangegeven voor welk doel de categorieën Wjsg-gegevens verwerkt mogen worden. Dat betekent dat de verwerking van gegevens alleen is toegestaan wanneer dit nodig is voor het specifieke doel dat voor de betreffende categorie Wjsg-gegevens in de Wjsg is vastgelegd. De verdere verwerking van Wjsg-gegevens voor andere doelen dan waarvoor ze verzameld zijn, is uitsluitend mogelijk wanneer dit expliciet is vastgelegd in de Wjsg of gelieerde wetgeving als het Besluit justitiële en strafvorderlijke gegevens ('Bjsg').

Justitiële gegevens mogen uitsluitend worden verwerkt ten behoeve van een goede strafrechtspleging.

Strafvorderlijke gegevens mogen uitsluitend worden verwerkt indien dit noodzakelijk is voor een goede vervulling van de taak van het OM of het nakomen van een andere wettelijke verplichting.

Gegevens in *persoonsdossiers* worden uitsluitend verwerkt met als doel de bevordering van een juiste toepassing van het strafrecht.

Tenuitvoerleggingsgegevens worden uitsluitend verwerkt indien dit noodzakelijk is voor een goede vervulling van een wettelijke taak of het nakomen van een andere wettelijke verplichting.

Gerechtelijke strafgegevens worden slechts verwerkt voor zover dit noodzakelijk is voor de rechtspraak.

4.3.3.2 Het ter beschikking stellen of verstrekken van Wjsg-gegevens

Net als de Wpg kent de Wjsg een gesloten verstrekkingsregime. Dit betekent dat uitsluitend gegevens mogen worden verstrekt aan derden wanneer dit mogelijk is op grond van een wettelijke bepaling in de Wjsg. Welke verstrekkingsmogelijkheden er zijn hangt af van de categorie Wjsg-gegevens die wordt verwerkt. Hieronder wordt per categorie Wjsg-gegeven nader ingegaan op de verstrekkingsmogelijkheden.

Justitiële gegevens:

Justitiële gegevens mogen uitsluitend verstrekt worden wanneer hiervoor een mogelijkheid is opgenomen in de Wjsg. In de Wjsg zijn een aantal bepalingen opgenomen die een dwingend karakter hebben en waaruit duidelijk blijkt aan wie en voor welk doel de justitiële gegevens verstrekt mogen worden.

Justitiële gegevens worden verstrekt aan (artikel 8 Wjsg):

- Nederlandse rechterlijke ambtenaren ten behoeve van de rechtspleging;
- De Minister van Justitie en Veiligheid ten behoeve van de strafrechtspleging;
- Lichamen of personen die op grond van artikel 257ba WvSv strafbeschikkingen mogen uitvaardigen ten behoeve van het uitoefenen van die bevoegdheid. De gegevens worden uitsluitend verstrekt t.b.v. de delicten waarop hun bevoegdheid betrekking heeft.

Naast deze verstrekkingsmogelijkheden, zijn in het Bjsg nog personen en instanties aangewezen aan wie voor een goede taakuitoefening justitiële gegevens verstrekt mogen worden. Aan de hand van het Bjsg dient dan ook beoordeeld te worden of aan een bepaald(e) persoon of instantie voor een bepaald doel justitiële gegevens verstrekt mogen worden.

Strafvordelijke gegevens

De mogelijkheden voor het verstrekken van strafvorderlijke gegevens zijn in de Wjsg opgedeeld in twee verschillende categorieën: het verstrekken van gegevens voor doelen gelegen binnen de strafrechtspleging en het verstrekken van gegevens voor buiten de strafrechtspleging gelegen doelen. Voor beide categorieën geldt dat de gegevens

alleen verstrekt mogen wanneer dit nodig is met het oog op een zwaarwegend algemeen belang.

Voor binnen de strafrechtspleging gelegen doelen mogen gegevens worden verstrekt aan:

- Nederlandse rechterlijke ambtenaren;
- De Minister van Justitie en Veiligheid;
- Lichamen of personen aan wie krachtens artikel 257ba WvSv de bevoegdheid is toegekend een strafbeschikking uit te vaardigen;
- Ambtenaren van politie als bedoeld in artikel 2 onder a Pw en ambtenaren van politie als bedoeld in artikel 2, onder c en d, voor zover zij zijn aangesteld voor de uitvoering van de politietaak;
- Ambtenaren als bedoeld in artikel 141 onderdeel c en d WvSv;
- Buitengewone opsporingsambtenaren als bedoeld in artikel 142 lid 1 WvSv;
- Instanties die belast zijn met de tenuitvoerlegging van rechterlijke beslissingen of handelingen, beslissingen van de officier van justitie dan wel van vrijheidsbenemende straffen of maatregelen;
- Verwerkingsverantwoordelijken voor de verwerking van politiegegevens als bedoeld in artikel 1 lid 1 onderdeel f Wpg;
- Bewaarders als bedoeld in artikel 118 lid 1 en 2 WvSv.
- Strafvorderlijke gegevens worden daarnaast verstrekt aan de ambtenaren die de justitiële documentatie opstellen.

Het verstrekken van strafvorderlijke gegevens voor buiten de strafrechtspleging gelegen doelen is alleen mogelijk wanneer dit past binnen de taakuitoefening van het Openbaar Ministerie. Strafvorderlijke gegevens mogen dus niet worden verstrekt ten behoeve van het belang dat een derde daarbij heeft.

Voor de verstrekking voor buiten de strafrechtspleging gelegen doelen is een limitatieve opsomming gegeven van de doelen waarvoor de gegevens verstrekt mogen worden.

Strafvorderlijke gegevens kunnen uitsluitend worden verstrekt voor één van de volgende doelen:

- Het voorkomen en opsporen van strafbare feiten;
- Het handhaven van de orde en veiligheid;
- Het uitoefenen van toezicht op het naleven van regelgeving;
- Het nemen van een bestuursrechtelijke beslissing;
- Het beoordelen van de noodzaak tot het treffen van een rechtspositionele of tuchtrechtelijke maatregel;
- Het verlenen van hulp aan slachtoffers en anderen die bij een strafbaar feit betrokken zijn, of
- Het verrichten van een privaatrechtelijke rechtshandeling door een persoon of instantie die met een publieke taak is belast.

Persoonsdossiers

Afschriften van de rapporten die zijn opgenomen in persoonsdossiers kunnen op verzoek verstrekt worden aan de volgen personen of instanties:

- Aan wie: Nederlandse rechterlijke ambtenaren.
  Doel: ten behoeve van een goede rechtspleging, de vervolging en berechting van strafbare feiten, de tenuitvoerlegging van straffen of maatregelen en het geven van advies over een gratieverzoek;
- Aan wie: Selectiefunctionarissen en hoofden van de inrichtingen waar de aan een persoon opgelegde straf of maatregel ten uitvoer wordt gelegd.
  Doel: ten behoeve van de selectie of bejegening;
- Aan wie: Directeuren van de stichting en de reclasseringsinstellingen, bedoeld in artikel 1, onder b en c van de Reclasseringsregeling 1995, de reclasseringswerkers, bedoeld in artikel 6 lid 1 Reclasseringsregeling en de directeur of ressortsdirecteur van de raad voor de kinderbescherming.
  Doel: ten behoeve van het voorbereiden van enig rapport of het uitoefenen van enig toezicht;
- Aan wie: andere personen of instanties die in het Bjsg zijn benoemd.

Doel: ten behoeve van een juiste toepassing van het strafrecht.

Tenuitvoerleggingsgegevens

In de Wsjg is limitatief aangegeven onder welke voorwaarden en doelen tenuitvoerleggingsgegevens verstrekt mogen worden. Er is geen uitputtende opsomming van de personen of instanties aan wie verstrekt mag worden. Ook hier geldt dat de verstrekking nodig moet zijn met het oog op een zwaarwegend algemeen belang. Voor de uitleg over de betekenis voor een zwaarwegend algemeen belang wordt verwezen naar de uitleg onder 13.1.3.2.

Tenuitvoerleggingsgegevens kunnen worden verstrekt voor:

- De tenuitvoerlegging van een strafrechtelijke beslissing;
- De voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten;
- Schuldhulpverlening of resocialisatie van betrokkene;
- Bestuurlijk handelen of het nemen van een bestuursrechtelijke beslissing, of
- Het verlenen van hulp aan slachtoffers.

Let wel deze verstrekking kan alleen plaatsvinden wanneer:

1. Dit voor de ontvangende personen of instanties nodig is wegens een zwaarwegend algemeen belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte; en
2. De gegevens in zodanige vorm worden verstrekt dat zoveel mogelijk wordt voorkomen dat andere personen, dan de betrokkene, op basis van de gegevens geïdentificeerd kunnen worden.

Gerechtelijke strafgegevens

De verstrekking van gerechtelijke strafgegevens is anders geformuleerd dan bij de andere categorieën Wjsg-gegevens. Waar de Wjsg, in samenhang met het Bjsg, een limitatieve opsomming geeft van de bepalingen waaronder justitiële-, strafvorderlijke-,

tenuitvoerleggingsgegevens en persoonsdossiers verstrekt mogen worden, wordt bij gerechtelijke strafgegevens een meer open formulering gebruikt. Gerechtelijke strafgegevens mogen worden verstrekt wanneer dit gebeurt ten behoeve van de behandeling van strafzaken en de verstrekking in overeenstemming is met hetgeen hierover is bepaald in het Wetboek van Strafvordering, dan wel gelieerde wetgeving zoals de Wet herziening regels betreffende processtukken in strafzaken en het Besluit processtukken in strafzaken.

Verstrekking van Wjsg-gegevens ten behoeve van onderzoek

Wjsg-gegevens kunnen met het oog op de doelen waarvoor de categorieën Wjsg-gegevens dienen, verstrekt worden ten behoeve van beleidsinformatie en wetenschappelijk onderzoek en statistiek. Deze verstrekking mag enkel wanneer de uiteindelijke resultaten geen persoonsgegevens bevatten.

In het Bjsg zijn nadere regels opgenomen over het verstrekken van gegevens voor beleidsinformatie en wetenschappelijk en statistisch onderzoek. Daarin is vastgelegd dat verstrekking alleen kan plaatsvinden wanneer de betrokken onderzoeker daarvoor schriftelijke toestemming heeft gekregen van de betreffende verwerkingsverantwoordelijke. Dit is afhankelijk van welke categorie Wjsg-gegevens worden verstrekt: de Minister van Justitie en Veiligheid, Het College van procureurs-generaal of het bestuur van een gerecht.

Toestemming wordt uitsluitend verleend, wanneer:

- De beleidsinformatie, of het onderzoek een algemeen belang dient;
- De organisatie die de gegevens verstrekt niet onnodig wordt belast;
- De beleidsinformatie zonder de betrokken gegevens onvolledig is of het onderzoek zonder de betrokken gegevens niet kan worden uitgevoerd, en
- De persoonlijke levenssfeer van de betreffende personen niet onevenredig wordt geschaad.

Aan de toestemming kunnen aanvullende voorwaarden worden verbonden. De verleende toestemming geldt als machtiging tot het verstrekken van de omschreven gegevens.

De onderzoeker mag de personen op wie de Wjsg-gegevens betrekking hebben niet benaderen, tenzij dit uitdrukkelijk is toegestaan in de verleende toestemming. Toestemming voor het benaderen van de betrokken personen kan alleen worden verleend wanneer rechtstreeks benadering voor het onderzoek noodzakelijk is.

4.4 Samenvatting

Wet- en regelgeving	Scope	Kernpunten	Opmerkingen
AVG	De AVG regelt de voorwaarden voor de verwerking van persoonsgegevens en de rechten van betrokkenen.	De AVG formuleert algemene beginselen en grondslagen die leidend zijn voor een rechtmatige en verantwoorde verwerking van persoonsgegevens. Daarnaast stelt de AVG ten aanzien van specifieke categorieën persoonsgegevens (bijzondere persoonsgegeven	De AVG geeft de kaders voor een rechtmatige verwerking van persoonsgegevens. Daarbij dient een onderscheid gemaakt te worden tussen de trainingsfase en de toepassingsfase en het type verwerking dat daarbij plaatsvindt (initiële verzameling of verdere verwerking) met inachtneming van het doelbindingsbeginsel). Verder is de AVG bij de toepassing van spraakherkenning ook bepalend voor de omgang met verschillende categorieën persoonsgegevens die daarbij

		s, strafrechtelijke gegevens) aanvullende eisen.	verwerkt zullen worden (dat wil zeggen reguliere persoonsgegevens, bijzondere persoonsgegeven en strafrechtelijke gegevens).
Wpg	De Wpg bepaalt de regels voor het verzamelen en verder verwerken van politiegegevens voor het handhaven van de rechtsorde en het verlenen van hulp aan hen die deze behoeven (de politietaak).	De Wpg regelt onder meer de specifieke voorwaarden waaronder politiegegevens verwerkt mogen worden, de doorgifte en verstrekking van politiegegevens, rechten van betrokkenen en bewaartermijnen.	De Wpg is van toepassing op de verwerking van politiegegevens door bevoegde autoriteiten. De Wpg regelt daarmee het gebruik van politiegegevens in de context van spraakherkenning die wordt ingezet voor de uitvoer van de politietaak.
Wjsg	De Wjsg ziet toe op de verwerking van justitiële gegevens, strafvorderlijke gegevens, persoonsdossiers, tenuitvoerleggi	De Wjsg regelt onder meer de specifieke voorwaarden waaronder Wjsg-gegevens verwerkt mogen worden, de terbeschikkingstelling en	De Wjsg regelt de rechtmatige verwerking van justitiële en strafvorderlijke gegevens ten behoeve van een goede strafrechtspleging. De Wjsg regelt daarmee het gebruik van justitiële en strafvorderlijke gegevens in de context van spraakherkenning die wordt

	ngsgegevens, gerechtelijke gegevens.	verstrekking van Wjsg-gegevens, rechten van betrokkenen en bewaartermijnen.	ingezet ten behoeve van een goede strafrechtspleging.

5 Juridisch kader overig

In het vorige hoofdstuk is het privacyrechtelijke kader dat een rol speelt bij de ontwikkeling en toepassing van spraakherkenning binnen het JenV-domein uiteengezet. We onderscheiden dit privacyrechtelijke kader van overige wetgeving die relevant is voor spraakherkenning in het JenV-domein. Hierbij moet onder andere worden gedacht aan de aankomende Europese AI-verordening, De modernisering van het Wetboek van Strafvordering en de Innovatiewet Strafvordering, de Algemene Wet Bestuursrecht en de Archiefwet. In dit hoofdstuk bespreken wij deze overige wetgeving.

5.1 Europese AI-Verordening

In april 2021 publiceerde de Europese Commissie (hierna: 'EC') het voorstel voor een verordening tot vaststelling van geharmoniseerde regels betreffende AI (wet op de artificiële intelligentie). Tegen de achtergrond van de razendsnelle ontwikkeling van AI en de impact van deze technologie op de mens en samenleving, streeft de EC er met deze regelgeving naar de invoering van AI te bevorderen en gelijktijdig de risico's te adresseren.

De Europese concept AI-verordening (AIV) stelt geharmoniseerde regels vast voor het in de handel brengen, in gebruik stellen en gebruiken van AI-systemen in de Unie. Daarbij heeft de EC bepaalde onacceptabele praktijken op het gebied van AI verboden, terwijl zij voor AI-systemen met een hoog risico specifieke voorschriften en verplichtingen voorschrijft. Bovendien bevat de AI-verordening specifieke geharmoniseerde transparantievoorschriften voor AI-systemen die zijn ontworpen om met natuurlijke personen te interacteren, systemen voor het herkennen van emoties en systemen voor biometrische categorisering evenals AI-systemen die worden gebruikt om beeld-, audio of video-inhoud te genereren of manipuleren.

5.1.1 Verboden praktijken op het gebied van AI

De concept AI-Verordening erkent dat naast de vele nuttige toepassingen, AI ook kan worden misbruikt en een nieuwe en krachtige bron voor manipulatie, uitbuiting en sociale

controle kan vormen.[58] Deze praktijken zijn in strijd met de basiswaarden die centraal staan in de EU, namelijk eerbied voor de menselijke waardigheid, respect voor grondrechten, vrijheid, gelijkheid, democratie en de rechtsstaat.[59]

Tegen deze achtergrond verbiedt de concept AI-Verordening onder meer bepaalde praktijken op het gebied van AI (artikel 1 sub a AIV). Deze verboden praktijken op het gebied van AI worden nader uitgewerkt in artikel 5 concept AI-Verordening. Ten aanzien van de toepassing van AI binnen het JenV-domein is hierbij met name het verbod in beginsel op het gebruik van biometrische systemen voor de identificatie op afstand in real time in openbare ruimten voor rechtshandhavingsdoeleinden relevant (artikel 5 lid 1 AIV).

Zoals in paragraaf 2.2.1. is besproken, omvat spraaktechnologie verschillende specifieke toepassingen, waaronder spraakherkenning en sprekerherkenning. Waar spraakherkenning uitsluitend gericht is op de daadwerkelijke omzetting van spraak naar tekst zonder daarbij de identiteit van de spreker(s) te bepalen, richt sprekerherkenning zich juist op de identificatie van sprekers. Het gevolg hiervan is dat de toepassing van sprekerherkenning in real time in openbare ruimten met het oog op rechtshandhaving in beginsel verboden is. Dit verbod geldt dus niet voor de toepassing van spraakherkenning binnen het JenV-domein zoals aan de orde in dit onderzoek: spraakherkenning met als doel autotranscriptie.

5.2 Juridisch kader voor hoog-risico AI-systemen

5.2.1.1 Classificatie van hoog-risico AI-systemen

Het grootste deel van de concept AI-Verordening ziet toe op de regulering van AI-systemen met een hoog risico. Artikel 6 bepaalt dat dit AI-systemen zijn die:

- Bedoeld zijn om te worden gebruikt als veiligheidscomponent van een product of zelf producten zijn die vallen on de in de bijlage II van de draft AI-Verordening

[58] Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van de geharmoniseerde regels betreffende artificiële intelligentie (Wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie.
[59] European Union. Aims and values. Geraadpleegd op 16 september 2022, van https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en.

opgenomen harmonisatiewetgeving (bijv. luchtvaartapparatuur, speelgoed en medische apparaten); of

- Opgesomd worden in de bijlage III van de concept AI-Verordening.

Hoog risico AI-systemen die in het kader van dit rapport met name relevant zijn, worden onder bijlage III van de concept AI-Verordening geschaard onder de toepassingsgebieden van:

- biometrische identificatie en categorisering van natuurlijke personen (6 lid 1 AIV)
    - Hieronder vallen AI-systemen die bedoeld zijn om te worden toegepast ten behoeve van de biometrische identificatie op afstand van natuurlijke personen in real time en achteraf.
- rechtshandhaving (6 lid 6 AIV)
    - Hieronder vallen onder meer AI-systemen die bedoeld zijn om door rechtshandhavingsautoriteiten gebruikt te worden voor:
        - uitvoeren van individuele risicobeoordelingen van natuurlijke personen.
        - leugendetectie of de vaststelling van de emotionele toestand van een natuurlijk persoon.
        - de beoordeling van de betrouwbaarheid van bewijsmateriaal tijdens het onderzoek naar of de vervolging van strafbare feiten
        - het voorspellen van een daadwerkelijk of potentieel strafbaar feit dat (opnieuw) zal worden gepleegd, op basis van de profilering van natuurlijke personen.
        - het uitvoeren van misdaadanalyses met betrekking tot natuurlijke personen, waardoor rechtshandhavingsautoriteiten complexe gerelateerde en ongerelateerde grote datareeksen kunnen doorzoeken die beschikbaar zijn in verschillende databronnen of verschillende data-indelingen om onbekende patronen op te sporen of verborgen relaties te ontdekken in de gegevens.
- rechtsbedeling en democratische processen (6 lid 8 AIV).

- Hieronder vallen AI-systemen die bedoeld zijn om ondersteuning te bieden aan rechterlijke instanties bij het onderzoeken en uitleggen van feiten en de wet en het toepassen van het recht in een concrete casus.

Voor al deze hoog-risico systemen gelden een aantal vereisten waaraan voldaan dient te worden in lijn met hoofdstuk 2 van de concept AI-Verordening. We lichten deze hieronder toe.

5.2.1.2 Voorschriften voor hoog-risico AI-systemen

Artikel 8 lid 1 van de draft AI-Verordening bepaalt dat AI-systemen met en hoog risico moeten voldoen aan de voorschriften die daarvoor in het bijzonder zijn voorgeschreven.

Systeem voor risicobeheer (artikel 9 AIV)

Artikel 9 lid 1 draft AI-Verordening bepaalt dat een systeem voor risicobeheer wordt vastgesteld, uitgevoerd, gedocumenteerd en in stand wordt gehouden voor hoog risico AI-systemen. Meer in het bijzonder omvat dit systeem de volgende verplichtingen:

- Het vaststellen en analyseren van de bekende en te voorziene risico's die gepaard gaan met elk AI-systeem met een hoog risico;
- Het doen van een inschatting en evaluatie van de risico's die zich kunnen voordoen wanneer het hoog risico AI-systeem wordt gebruikt in overeenstemming met het beoogde doel van het systeem en in een situatie van redelijkerwijs te voorzien misbruik;
- Het doen van een evaluatie van andere risico's die zich kunnen voordoen op basis van de analyse van de data die zijn verzameld door het systeem voor monitoring na het in de handel brengen van het betreffende hoog risico AI-systeem; en
- Het vaststellen van geschikte risicobeheersingsmaatregelen.

Wat betreft het vaststellen van geschikte beheersmaatregelen bepaalt artikel 9 lid 3 draft AI-Verordening dat naar behoren rekening dient te worden gehouden met de effecten en mogelijke wisselwerkingen die voortvloeien uit de gecombineerde toepassing van de in hoofdstuk 2 van de draft AI-Verordening bepaalde voorschriften.

Verder bepaalt artikel 9 lid 4 AIV dat de maatregelen zodanig dienen te zijn dat eventuele restrisico's in verband met elk gevaar en het totale restrisico van het betreffende hoog risico AI-systeem als aanvaardbaar kan worden aangemerkt. Bovendien dient de gebruiker op de hoogte te worden gesteld van deze restrisico's.

Bij het vaststellen van de maatregelen moet rekening worden gehouden met de te verwachten technische kennis, ervaring, scholing en opleiding van de gebruiker en de omgeving waarin het systeem wordt gebruikt. In het bijzonder moet de aanbieder:

- De risico's zo veel mogelijk uitsluiten of beperken door een adequaat ontwerp en adequate ontwikkeling;
- Adequate maatregelen voor beperking en controle voor risico's die niet kunnen worden uitgesloten treffen; en
- Toereikende informatie aan de gebruiker bieden over het gebruik van het systeem. Hoe toereikende informatie kan worden gegarandeerd, wordt nader uitgewerkt in artikel 13 draft AI-Verordening en zal in het navolgende uitgebreider aan bod komen.

AI-systemen met een hoog risico worden aan de hand van vooraf vastgestelde standaarden en probabilistische drempels getest met het oog op het vaststellen van de juiste beheersmaatregelen. De testprocedures behoeven nier verder te gaan dan wat noodzakelijk is om het beoogde doel van het hoog risico AI-systeem te verwezenlijken en worden tenuitvoergelegd in de loop van het ontwikkelingsproces of in ieder geval voorafgaand aan het in handel brengen van het betreffende systeem.

Data en databeheer (artikel 10 AIV)

Artikel 10 lid 1 AIV bepaalt dat hoog risico AI-systemen die gebruikmaken van technieken voor het trainen van modellen met data, dienen te worden ontwikkeld op basis van datareeksen voor training, validatie en tests die voldoen aan bepaalde kwaliteitscriteria. Als zodanig worden datareeksen voor training, validatie en tests onderworpen aan 'passende praktijken' op het gebied van databeheer (artikel 10 lid 2 AIV).

Hiermee wordt beoogd dat datareeksen voor training, validatie en tests in lijn met artikel 10 lid 3 AIV relevant, representatief, foutenvrij en volledig zijn. Daarnaast dienen de relevante datareeksen passende statistische kenmerken te omvatten. Bij dit alles wordt, op grond van artikel 10 lid 4 AIV rekening gehouden met de eigenschappen of elementen die specifiek zijn voor een bepaalde geografische, functionele of gedragsomgeving waarin het AI-systeem moet worden gebruikt.

Technische documentatie (artikel 11 AIV)

Voordat een hoog risico AI-systeem in de handel wordt gebracht, in gebruik wordt gesteld of geactualiseerd, wordt technische documentatie over het systeem opgesteld (artikel 11 lid AIV). Aan de hand van deze technische documentatie moet de aanbieder aantonen dat het hoog risico AI-systeem in overeenstemming is met de voorschriften uit hoofdstuk 2 AIV die hierboven zijn besproken. Daarnaast dient de technische documentatie het voor nationale bevoegde autoriteiten en aangemelde instanties mogelijk te maken om over alle noodzakelijk informatie te beschikken om de overeenstemming van de betreffende hoog risico AI-systemen met voornoemde voorschriften te kunnen beoordelen.

De technische documentatie dient op grond van artikel 11 lid 1 AIV in ieder geval de elementen zoals opgenomen in bijlage IV te omvatten, namelijk:

- Een algemene beschrijving van het AI-systeem;
- Een gedetailleerde beschrijving van de elementen van het AI-systeem en van het proces voor de ontwikkeling ervan;
- Gedetailleerde informatie over de monitoring, werking en controle van het AI-systeem;
- Een gedetailleerde beschrijving van het systeem voor risicobeheer (artikel 9 AIV);
- Een beschrijving van de wijzigingen die tijdens de levensduur van het systeem worden aangebracht.

- Een lijst van de geharmoniseerde normen die volledig of gedeeltelijk worden toegepast en waarvan de referenties zijn gepubliceerd in het Publicatieblad van de Europese Unie;
- Een exemplaar van de EU-conformiteitsverklaring; en
- Een gedetailleerde beschrijving van het ingevoerde systeem voor de evaluatie van de prestaties van het AI-systeem nadat het in de handel is gebracht (artikel 61 AIV).

Registratie (artikel 12 AIV)

Hoog risico AI-systemen dienen overeenkomstig artikel 12 lid 1 AIV op een zodanige wijze te worden ontworpen en ontwikkeld dat zij de automatische registratie van gebeurtenissen (logging) tijdens de werking van het systeem mogelijk maken. Deze loggingscapaciteiten dienen in overeenstemming te zijn met erkende normen of gemeenschappelijke specificaties en behoren een mate van traceerbaarheid van de werking van het AI-systeem tijdens de levensduur ervan te waarborgen die passend is voor het beoogde doel van het systeem (artikel 12 lid 2 AIV).

Transparantie en informatieverstrekking aan gebruikers (artikel 13 AIV)

Artikel 13 lid 1 AIV bepaalt dat hoog risico AI-systemen zodanig dienen te worden ontworpen en ontwikkeld dat de werking ervan voldoende transparant is om gebruikers in staat te stellen de output van het systeem te interpreteren en op passende wijze te gebruiken. Daarnaast dienen hoog risico AI-systemen voorzien te worden van gebruiksinstructies in een passend digitaal of ander formaat. Dergelijke gebruiksinstructies behoren beknopte, volledige, juiste en duidelijke informatie te bevatten die relevant, toegankelijk en begrijpelijk is voor de betreffende gebruikers. Artikel 13 AIV bepaalt dat deze informatie in ieder geval het volgende dient te omvatten:

- De identiteit en de contactgegevens van de aanbieder;
- De kenmerken, capaciteiten en beperkingen van de prestaties van het betreffende hoog risico systeem. Dit betreft onder meer het beoogde doel, (eventuele bekende en te voorziene omstandigheden die een effect kunnen hebben op) de mate van nauwkeurigheid, robuustheid en cyberbeveiliging. Verder omvat dit ook de

eventuele bekende of te voorziene omstandigheden in verband met het gebruik van het hoog risico AI-systeem in overeenstemming met het beoogde doel ervan of in een situatie van redelijkerwijs te voorzien misbruik, die kunnen leiden tot risico's voor de gezondheid en veiligheid of de grondrechten; de prestaties van het betreffende hoog risico AI-systeem met betrekking tot de personen en groepen personen voor wie het systeem moet worden gebruikt; en eventuele specificaties voor de inputdata of eventuele andere relevante informatie met betrekking tot de gebruikte datareeksen voor training, validatie en tests;

- De wijzigingen en prestaties van het hoog risico AI-systeem die vooraf door de aanbieder zijn bepaald op het moment van de eerste conformiteitsbeoordeling;
- De maatregelen voor menselijk toezicht in overeenstemming met artikel 14 AIV, waaronder ook de technische maatregelen die zijn genomen om de interpretatie van de output van AI-systemen door gebruikers te vergemakkelijken;
- De verwachte levensduur van het hoog risico AI-systeem en eventuele noodzakelijke maatregelen voor onderhoud en verzorging om de goede werking van het betreffende AI-systeem te waarborgen.

Menselijk toezicht (artikel 14 AIV)

Hoog risico AI-systemen dienen op grond van artikel 14 AIV zodanig te worden ontworpen en ontwikkeld dat menselijk toezicht door natuurlijke personen op het functioneren van het betreffende systeem op een doeltreffende wijze kan worden uitgeoefend in de periode dat het systeem wordt gebruikt. Dit toezicht is erop gericht om risico's voor de gezondheid, veiligheid of grondrechten te voorkomen of beperken. Deze risico's kunnen voorkomen wanneer het betreffende AI-systeem wordt gebruikt in overeenstemming met het beoogde doel ervan of in een situatie van redelijkerwijs te voorzien misbruik.

Op grond van artikel 14 lid 3 AIV moet de aanbieder een inschatting maken van de risico's en waar technisch haalbaar voorzieningen treffen in het systeem zelf voor menselijk toezicht en/of aangeven welke maatregelen de gebruiker moet treffen.

De natuurlijke personen die voor het menselijk toezicht verantwoordelijk zijn, dienen met een oog op de omstandigheden op grond van artikel 14 lid 4 AIV in staat te zijn om het volgende te doen:

- De capaciteiten en beperkingen van het betreffende AI-systeem volledig begrijpen en de werking ervan naar behoren kunnen monitoren, zodat een foutieve werking zo snel mogelijk kan worden gedetecteerd en aangepakt;
- Bewust zijn van de neiging om automatisch of te veel te vertrouwen op de output van een hoog risico AI-systeem, met name voor die hoog risico AI-systemen die worden gebruikt om informatie of aanbevelingen te verstrekken voor door natuurlijke personen te nemen beslissingen;
- De output van het AI-systeem met een hoog risico juist interpreteren, in het bijzonder rekening houdend met de kenmerken van het systeem en de beschikbare instrumenten en methoden voor interpretatie;
- In alle specifieke situaties kunnen besluiten om het AI-systeem niet te gebruiken of de output ervan op andere wijze te negeren, terzijde te schuiven of terug te draaien;
- Ingrijpen in de werking van het AI-systeem of het systeem onderbreken door middel van een stopknop of een vergelijkbare procedure.

Met name gezien de relevantie van hoog risico AI-systemen voor de biometrische identificatie en categorisering van natuurlijke personen (bijlage III lid 1 sub a AIV), verdient het opmerking dat voornoemde maatregelen op grond van artikel 14 lid 5 AIV zodanig dienen te zijn dat zij waarborgen dat door de gebruiker geen maatregelen worden getroffen of beslissingen worden genomen op basis van de identificatie door het systeem, tenzij deze door ten minste twee natuurlijke personen zijn geverifieerd en bevestigd.

Nauwkeurigheid, robuustheid en cyberbeveiliging (artikel 15 AIV)

Artikel 15 lid 1 AIV bepaalt dat AI-systemen met een hoog risico op zodanige wijze dienen te worden ontworpen en ontwikkeld zodat deze, met het oog op hun beoogde doel, een passend niveau van nauwkeurigheid, robuustheid en cyberbeveiliging bieden en ook waarborgen dan prestaties gedurende de levensduur met betrekking tot deze aspecten

consistent zijn. Wat deze niveaus van en relevante maatstaven voor nauwkeurigheid zijn, dient op grond van artikel 15 lid 2 AIV te worden vermeld in de bijbehorende gebruiksaanwijzingen van het betreffende hoog risico AI-systeem.

Artikel 15 lid 3 AIV bepaalt dat hoog risico AI-systemen bestand moeten zijn tegen fouten en onregelmatigheden die zich kunnen voordoen binnen het systeem of de omgeving waarin het systeem wordt gebruikt. Dergelijke fouten en onregelmatigheden doen zich met name voor als gevolg van de interactie van de betreffende systemen met natuurlijke personen of andere systemen. Daarnaast bepaalt artikel 15 lid 3 AIV ten aanzien van de robuustheid van hoog risico AI-systemen dat deze kan worden gerealiseerd door middel van technische oplossingen voor redundantie, die plannen voor de back-up of de veiligheid bij defecten kunnen omvatten. Bovendien is het op grond van artikel 15 lid 4 AIV vereist dat hoog risico AI-systemen bestand zijn tegen pogingen van ongeautoriseerde derden om het gebruik of de prestaties van het systeem te wijzigen door gebruik te maken van de kwetsbaarheden van het systeem. De technische oplossingen die hiertoe in het leven worden geroepen sluiten aan op de relevante omstandigheden en risico's.

5.2.2 Juridisch kader voor overige AI-systemen

Ten aanzien van AI-systemen die voor interactie met natuurlijke personen zijn bestemd, geldt op grond van artikel 52 lid 1 draft AI-Verordening dat aanbieders van deze systemen ervoor dienen te zorgen dat deze systemen zodanig zijn ontworpen en ontwikkeld dat natuurlijke personen worden geïnformeerd dat zij interacteren met een AI-systeem, tenzij omstandigheden en de gebruikscontext dit duidelijk maken. Deze verplichting geldt niet voor bij wet toegestane AI-systemen voor het opsporen, voorkomen, onderzoeken en vervolgen van strafbare feiten, tenzij die systemen voor het publiek beschikbaar zijn om een strafbaar feit te melden.

Gezien de relevantie in het kader van dit rapport, geldt bovendien op grond van artikel 52 lid 3 AIV dat gebruikers van een emotieherkenningssysteem of een of een biometrisch indelingssysteem de daaraan blootgestelde natuurlijke personen op de hoogte dienen te stellen van de werking van het systeem. Deze verplichting is wederom niet van toepassing

waar voor biometrische indeling gebruikte AI-systemen bij wet zijn toegestaan om strafbare feiten op sporen, te voorkomen en te onderzoeken.

5.3 Modernisering Wetboek van Strafvordering & Innovatiewet Strafvordering

Vooruitlopend om de complete modernisering van het Wetboek van Strafvordering zijn nu al enkele bepalingen ingevoerd die de strafvordering moeten verbeteren via de Innovatiewet Strafvordering. Deze wet is sinds 1 oktober 2022 van kracht.

In het kader van dit rapport is met name afdeling 3 van de Innovatiewet Strafvordering 'Bewijs door opname van beeld, geluid, of beeld en geluid' relevant om te benoemen. Artikel 557 bepaalt namelijk dat in aanvulling op artikel 339 Wetboek van Strafvordering ook een opname van beeld, geluid, of beeld en geluid als wettig bewijsmiddel erkend wordt. Alhoewel een schriftelijke transcriptie bij het audio- of beeldmateriaal niet vereist is, is het met het oog op efficiëntie en accuraatheid en gelet op de toenemende kwaliteit van automatisch gegenereerde transcripties mogelijk dat de Innovatiewet Strafvordering impact heeft op de vraag naar spraakherkenning binnen de strafrechtpleging.

5.4 Algemene wet bestuursrecht

De Algemene wet bestuursrecht (hierna; 'Awb') is een Nederlandse wet die de algemene regels bevat voor de verhouding tussen overheid en burger. Hoewel een inhoudelijke bespreking van de Awb buiten de reikwijdte van dit rapport valt, is het van belang te benoemen dat deze wet onder andere het nemen van overheidsbesluiten regelt. Wanneer spraakherkenning een rol speelt in het nemen van besluiten kan de Awb dus relevant zijn.

Naast de wettelijke regels uit de Awb dient ook rekenign te worden gehouden met de algemene beginselen van behoorlijk bestuur (hierna: 'ABBB'):

- Beginselen voor het proces van voorbereiding en besluitvorming (zorgvuldige voorbereiding, fair-play beginsel en verbod van détournement de procedure);
- Beginselen voor motivering en inrichting van besluiten (draagkrachtige en kenbare motivering, en rechtszekerheid); en

- Beginselen ten aanzien van de inhoud van besluiten (rechtszekerheid- en vertrouwensbeginsel, gelijkheidsbeginsel, verbod van détournement de pouvoir, materiële zorgvuldigheid en evenredigheidsbeginsel).

5.5 Archiefwet

Overheidsorganen zijn verplicht om (een deel van de) door hen gegenereerde informatie (voor langere perioden) te bewaren. Welke vereisten en voorwaarden hieraan verbonden zijn, wordt in de Archiefwet, het Archiefbesluit en de Archiefregeling beschreven. Het doel van deze wet- en regelgeving is om belangrijke overheidsinformatie te behouden en toegankelijk te maken.

Omdat niet alle door overheidsorganisaties gegenereerde informatie even belangrijk wordt geacht, wordt in selectielijsten vastgelegd welke informatie bewaard dient te worden en voor welke periode. Zodra archiefbescheiden als 'te bewaren' worden aangemerkt, dienen deze op termijn naar een archiefbewaarplaats overgebracht te worden. Bewaartermijnen die hierbij gelden, variëren in duur. Daarnaast geldt dat wanneer de bewaartermijn is verlopen, overheden geacht worden de betreffende informatie te vernietigen. Overheidsorganen zijn dus niet alleen verplicht de onder hen berustende archiefbescheiden[60] in goede, geordende en toegankelijke staat te brengen en te bewaren, maar dienen ook te zorgen voor de vernietiging van de archiefbescheiden die daarvoor in aanmerking komen.

Ten aanzien van archivering binnen het JenV-domein geldt dat de minister van JenV is aangewezen als de zorgdrager, in de zin van artikel 1, onderdeel d, van de Archiefwet. Dit betekent dat de minister belast is met de zorg voor de archiefbescheiden en het ontwerpen en opstellen van selectielijsten voor zijn ministerie. Deze selectielijst – de Selectielijst van het Ministerie van Justitie en Veiligheid en rechtsvoorgangers vanaf 5 mei 1945[61] – geeft een opsomming van de taken van JenV en een systematisch overzicht van de categorieën

[60] Deze term wordt ruim geïnterpreteerd en omvat niet enkel de documenten die zijn gearchiveerd, maar alle informatie die ambtenaren vanuit hun functie opmaken of ontvangen, in de context van het handelen van het overheidsorgaan.
[61] Selectielijst van het Ministerie van Justitie en Veiligheid en rechtsvoorgangers vanaf 5 mei 1945. Geraadpleegd op 16 september 2022, van https://www.nationaalarchief.nl/sites/default/files/field-file/Selectielijst%20JenV%20vastgesteld%20Stcrt%202021%2017848.pdf.

archiefbescheiden met vermelding van bewaartermijnen. Zonder deze selectielijst mag JenV niet overgaan tot vernietiging dan wel overbrenging van archiefbescheiden. Waar relevant in het kader van dit rapport, wordt specifiek verwezen naar dit selectiebesluit.[62]

Archiefbescheiden bevatten veelal persoonsgegevens, waarop de AVG en de Uitvoeringswet AVG (hierna: 'UAVG') van toepassing zijn. Waar het archivering en de bescherming van persoonsgegevens betreft, bestaat een zeker spanning tussen beide wetten, zeker gezien het belang dat in de AVG wordt toegekend aan het uitgangspunt van dataminimalisatie in de zin van artikel 5 AVG. Het gevolg hiervan is dat overheidsorganen in de praktijk er vaak toe gezet worden het belang van archivering af te wegen tegen het belang van bescherming van persoonsgegevens.

Momenteel wordt door de Rijksoverheid gewerkt aan vernieuwing. Met het oog op het voorgaande, heeft de Autoriteit Persoonsgegevens (hierna: AP') in het kader van deze vernieuwing geadviseerd de beginselen van gegevensbescherming zoals die in de AVG zijn opgenomen, beter in de nieuwe wetgeving te integreren.[63] Hiermee beoogt de AP ervoor te zorgen dat overheidsorganisaties in overeenstemming met de Archiefwet handelen ook direct voldoen aan de vereisten die in de AVG zijn neergelegd.

In het kader van dit rapport speelt de Archiefwet met name een relevante rol waar het de juridische aspecten rondom de opslag van door spraakherkenning gegenereerde overheidsdocumenten betreft.

5.6 Wet open overheid

De Wet open overheid (hierna: 'Woo') is op 1 mei 2022 in werking getreden. Deze wet vervangt de Wet openbaarheid van bestuur (hierna: 'Wob') en ziet toe op de bescherming van het recht op toegang, dat wil zeggen het recht dat eenieder heeft op toegang tot publieke informatie zonder daartoe een belang te hoeven stellen, behoudens bij deze wet

[62] Het verdient hierbij opmerking dat de nationale politie een eigen selectielijst heeft waarvoor de korpschef verantwoordelijk is.
[63] Autoriteit Persoonsgegevens (2019). Advies over het concept voor een wetsvoorstel Modernisering Archiefwet (Archiefwet 2021). Geraadpleegd op 16 september 2022, van https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_modernisering_archiefwet.pdf.

gestelde beperkingen (artikel 1.1. Wet open overheid). Het grote verschil tussen de huidige Woo en de Wob betreft de actieve openbaarmaking van overheidsinformatie. Voor passieve openbaarmaking (openbaarmaking op verzoek) volgt de Woo vrijwel geheel de Wob.

Hoewel deze wet niet direct toeziet op de verantwoorde toepassing van spraakherkenning binnen JenV, kan deze wet wel een rol spelen bij de openbaarmaking van middels spraakherkenning gegenereerde schriftelijk vastgestelde publieke stukken.

5.7 Samenvatting

Het hierboven geschetste juridisch kader omvat een uitgebreide omschrijving van alle relevante vereisten waar rekening mee dient te worden gehouden bij de verantwoorde toepassing van spraakherkenning. De kern van dit juridisch kader wordt in de tabel hieronder samengevat en weergegeven.

Wet- en regelgeving	**Scope**	**Kernpunten**	**Opmerkingen**
Concept AI-Verordening	De Verordening stelt regels vast voor het in handel brengen, in gebruik stellen en gebruiken van AI-systemen in de Unie.	De concept AI-Verordening classificeert AI-systemen in vier risicocategorieën: onacceptabel risico, hoog risico, beperkt risico en weinig tot geen risico. Voor elk van deze risicocategorieën regelt de Verordening de toelaatbaarheid van deze systemen en de voorwaarden	Spraakherkenning die wordt toegepast in het JenV-domein kan afhankelijk van de context binnen de categorie 'hoog risico vallen'. De Verordening stelt ten aanzien hoog risico AI-systemen een aantal specifieke voorschriften (*Systeem voor risicobeheer,* Data en databeheer, Technische

		waaronder zij toelaatbaar worden geacht.	documentatie, Registratie, Transparantie en informatieverstrekking, Menselijk toezicht, Nauwkeurigheid, robuustheid en cyberbeveiliging) die bij de toepassing van spraakherkenning binnen JenV in acht genomen moeten worden.
Innovatiewet strafvordering	De Innovatiewet strafvordering heeft tot doel om vooruitlopend op het bredere moderniseringstraject strafvordering de strafvordering te verbeteren.	De Innovatiewet Strafvordering regelt dat een opname van beeld, geluid, of beeld en geluid als wettig bewijsmiddel erkend wordt.	Wanneer beeld en geluid onderdeel worden van het strafdossier kan de behoefte ontstaan tot transcriptie daarvan (in aanvulling op het audiovisuele materiaal zelf).
Awb & ABBB	De Awb regelt de verhouding tussen overheid en burger. De ABBB bepalen de algemene (ongeschreven)	De Awb bevat regels voor het nemen van rechtsgeldige besluiten door de overheid en de rechtsmiddelen die daar tegen openstaan.	Waar spraakherkenning een rol speelt binnen de besluitvormingsprocedures van bestuursorganen binnen het JenV-

	gedragsregels in overeenstemming waarmee bestuursorganen zich moeten gedragen.	Naast de wettelijke regels, is op de interactie tussen overheid en burgers/bedrijfsleven ook een reeks ongeschreven gedragsregels – de ABBB – van toepassing. Deze omvatten beginselen omtrent procedures, motivering en inrichting, en inhoud.	domein, spelen de Awb en de ABBB een rol.
Archiefwet	De Archiefwet regelt het beheer van en de toegang tot overheidsarchieven.	De Archiefwet, het Archiefbesluit en de Archiefregeling bepalen de voorwaarden en vereisten rondom het behoud en de toegankelijkheid van overheidsinformatie. Selectielijsten stellen vast welke overheidsinformatie gearchiveerd dient te worden.	De Archiefwet speelt in het kader van spraakherkenning met name een relevante rol waar het de juridische aspecten rondom de opslag van door spraakherkenning gegenereerde overheidsdocumenten betreft.

		Voor JenV bestaat een aparte selectielijst, de Selectielijst van het Ministerie van Justitie en Veiligheid en rechtsvoorgangers vanaf 5 mei 1945.	
Wet open overheid	De Woo is van toepassing op bestuursorganen en andere overheidsorganen overeenkomstig artikel 2.2. Woo.	De Woo ziet toe op de bescherming van het recht op toegang (dat wil zeggen het recht dat eenieder in heeft op toegang tot publieke informatie zonder daartoe een belang te hoeven stellen.	De Woo kan een rol spelen bij de openbaarmaking van publieke informatie vastgesteld door middel van spraakherkenning.

6 Juridische analyse van spraakherkenning binnen het JenV-domein

In dit rapport onderzoeken we onder welke juridische voorwaarden spraakherkenning en autotranscriptie verantwoord toegepast kunnen worden binnen het JenV-domein. We beantwoorden deze vraag aan de hand van een aantal deelvragen die met name toezien op de vereisten en beperkingen die juridische kaders stellen aan:

- het verkrijgen van toestemming voor het gebruik van autotranscriptie;
- het opslaan van integrale audio-opnames van gesprekken en letterlijke transcripties daarvan;
- het trainen van spraakherkenning met trainingsdata; en
- het afnemen van spraaktechnologie uit de markt en samenwerking met derden (zie bijlage 1).

Dit hoofdstuk beantwoordt de betreffende deelvragen op basis van het juridisch kader dat is geschetst in de hoofdstukken 4 en 5.[64]

6.1 Vooraf: training en toepassing

Voordat we de grondslagen voor het vaststellen van de legitimiteit van verwerkingsactiviteiten in de context van spraakherkenning uiteenzetten, is het van belang een duidelijk onderscheid te maken tussen het trainen van een spraakherkenningssysteem en de praktische toepassing ervan. Zoals uit paragrafen 2.2.1. en 2.2.2. blijkt, zijn het trainen en gebruiken van spraakherkenningsmodellen twee afzonderlijke activiteiten en daarmee twee afzonderlijke verwerkingsdoeleinden.

Omdat de verwerking een ander doel dient, is er mogelijk ook een ander juridisch kader van toepassing en kan de grondslag voor de verwerking verschillen. Bij de bepaling van de legitimiteit van verwerkingsactiviteiten maken we daarom, waar relevant, onderscheid tussen: 1) het trainen en hertrainen van een spraakherkenningssysteem en 2) de toepassing

[64] Het feit dat een JenV-organisatie grondwettelijk onafhankelijk is, heeft geen invloed op de conclusies uit dit rapport voor wat betreft de juridisch verantwoorde inzet van spraakherkenning.

hiervan. Paragraaf 6.2 en 6.3 beperken zich tot de toepassing van spraakherkenning. De juridische voorwaarden omtrent het (her)trainen van spraakherkenningssystemen komen in paragraaf 6.4. nader aan bod.

6.2 Wettelijke grondslagen voor verwerking

De grondslagen voor de verwerking van persoonsgegevens in de context van spraakherkenning in het domein van justitie en veiligheid liggen primair in de AVG, de Wpg en de Wjsg. Omdat de daadwerkelijke rechtmatigheid van de verwerking afhangt van de concrete toepassing, beantwoorden wij de vraag omtrent de rechtmatigheid van de gegevensverwerkingen bij spraakherkenning in belangrijke mate aan de hand van de *use cases* uit hoofdstuk 3.

6.2.1 AVG

Zoals in paragraaf 4.1.2. uiteengezet bepaalt artikel 6 AVG dat de verwerking van persoonsgegevens enkel rechtmatig is voor zover een van de volgende grondslagen van toepassing is:

- Toestemming;
- Overeenkomst;
- Wettelijke plicht;
- Vitale belangen;
- Taak van algemeen belang/openbaar gezag;
- Gerechtvaardigde belangen.

Daarnaast omvat de AVG aanvullende vereisten voor de verwerking van bijzondere categorieën persoonsgegevens en strafrechtelijke gegevens.

In de *use case* beschreven in paragraaf 3.2. hebben we gekeken naar het gebruik van spraakherkenning door de Reclassering. De Reclassering valt onder de reikwijdte van de AVG. Dit betekent dat de verwekingsactiviteiten van de Reclassering in ieder geval gebaseerd moeten worden op één van de grondslagen uit artikel 6 AVG. Daarnaast gelden aanvullende vereisten bij de verwerking van bijzondere categorieën van persoonsgegevens of strafrechtelijke gegevens.

Hoewel *toestemming* in de door JenV gestelde deelvragen nadrukkelijk is aangehaald als een mogelijke grondslag, biedt zij zeer hoogstwaarschijnlijk géén geldige grondslag voor de verwerking van persoonsgegevens door de Reclassering. In hoofdstuk 4.2.2. is beschreven dat toestemming in de zin van artikel 6 lid 1 onder a aan strenge vereisten moet voldoen (vrijelijk gegeven, specifiek, geïnformeerd, en ondubbelzinnig). In het geval van de verwerking van persoonsgegevens door de Reclassering kan hieraan niet volledig worden voldaan. Met name de vrije verlening van de toestemming is problematisch. Wanneer de Reclassering persoonsgegevens verwerkt van bijvoorbeeld een dader van een strafbaar feit, heeft de betrokkene doorgaans weinig keuze over de verwerking van zijn persoonsgegevens. Daarom is toestemming - in de context van de Reclassering - doorgaans niet geschikt als juridische grondslag.

Op welke grondslagen de verwerkingen dan wel gebaseerd kunnen worden hangt af van de specifieke context waarin de verwerking plaatsvindt. Voor de Reclassering geldt dat zij moet kunnen onderbouwen dat de verwerking of: 1) noodzakelijk is in het kader van de uitvoering van de aan haar wettelijk opgedragen reclasseringstaak (6e AVG), of dat de verwerking noodzakelijk is met het oog op haar gerechtvaardigde belangen (6f AVG) (in dit geval een effectieve en efficiënte bedrijfsvoering). Uiteindelijk komt de argumentatie voor grondslag 6e en 6f AVG op hetzelfde neer: zonder gebruik te maken van spraakherkenning kan de Reclassering haar taken niet, of in ieder geval veel minder effectief en efficiënt uitvoeren. Argumenten hierbij zijn bijvoorbeeld dat spraakherkenning gebruiken voor auto-transcriptie completer, accurater en/of efficiënter is dan ‘fysieke transcriptie’.

6.2.2 Wpg

Voor de politie geldt dat zij spraakherkenning moet kunnen baseren op de uitvoering van haar politietaken. Wanneer de politie persoonsgegevens verwerkt ter uitoefening van de politietaak, kwalificeren deze persoonsgegevens als politiegegevens. Wanneer de politie spraakherkenning toepast ter uitoefening van de politietaak, vindt de verwerking van persoonsgegevens plaats ten behoeve van dat doel en onder de verwerkingsverantwoordelijkheid van de korpschef, bedoeld in artikel 27 van de Politiewet

2012 (artikel 1 sub f Wpg). Daarbij geldt dat politiegegevens enkel verwerkt mogen worden voor zover dit gebeurt met het oog op de uitoefening van de politietaak (artikel 1 sub a Wpg jo. artikel 3 Politiewet jo. artikel 3 lid 1 Wpg). De artikelen 8-13 Wpg bepalen welke specifieke verwerkingsactiviteiten hieronder vallen.

De toepassing van spraakherkenning kan op de volgende grondslagen worden gebaseerd:

- Artikel 8 Wpg - uitvoering van de dagelijkse politietaak (bijv. in het kader van het digitaal gesproken zakboekje of het operationeel centrum 112-meldkamer);
- Artikel 9 Wpg - onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (bijvoorbeeld in het geval van het verhoor).

Bovendien bepaalt de Wpg in artikel 5 over bijzondere categorieën politiegegevens, dat deze enkel mogen worden verwerkt voor zover dit onvermijdelijk is voor het doel van de verwerking, in aanvulling op de verwerking van andere politiegegevens betreffende de persoon en de gegevens voldoende zijn beveiligd.

Zoals in paragraaf 4.2.3. is uitgelegd ten aanzien van artikel 9 AVG, worden er bij de toepassing van spraakherkenning biometrische persoonsgegevens verwerkt. Deze gegevens kwalificeren niet per definitie als bijzondere categorieën persoonsgegevens. Daarnaast zal gezien de werking en de doeleinden waarvoor spraakherkenning door de politie wordt ingezet in beginsel geen sprake zijn van de verwerking van andere bijzondere categorieën politiegegevens. Dit moet per proces waarvoor spraakherkenning wordt ingezet worden getoetst. In de praktijk betekent dit dat wanneer spraakherkenning wordt gebruikt -bijvoorbeeld bij een verhoor- moet worden gekeken in hoeverre bijzondere persoonsgegevens worden gebruikt en of door het gebruik van spraakherkenning nieuwe risico's ontstaan. Dit kan bijvoorbeeld worden gedaan door het uitvoeren van een gegevensbeschermingseffectbeoordeling (GEB/DPIA) op een bestaand proces.

Wanneer wij de Wpg als grondslag nemen moet de politie dus kunnen onderbouwen dat transcriptie noodzakelijk is voor de goede uitvoering van de politietaak. Net als bij de

Reclassering moet de politie onderbouwen waarom het gebruik van spraakherkenning completer, accurater en/of efficiënter is dan de inzet van een verbalisant.

Het valt ook te betogen dat spraakherkenning een onderdeel vormt van een goede bedrijfsvoering: het maakt het werk van de politie effectiever, eenvoudiger en efficiënter. In dat geval zou de spraakherkenning toegepast worden in het kader van de interne bedrijfsvoering. Artikel 2 lid 2 sub b Wpg sluit verwerkingen in het kader van de interne bedrijfsvoering uit van het toepassingsbereik van de Wpg. Op dergelijke verwerkingen is dan niet de Wpg maar de AVG van toepassing. Het gaat bij dergelijke verwerkingsactiviteiten dan niet meer om de verwerking van persoonsgegevens ten behoeve van de uitvoering van de politietaak en de persoonsgegevens die worden verwerkt kwalificeren daarom niet als politiegegevens (denk bijvoorbeeld aan de verwerking van de persoonsgegevens van de agent in het geval van het digitaal gesproken zakboekje).

Per situatie of proces waarvoor JenV spraakherkenning inzet dient te worden beoordeeld of de verwerking gebaseerd moet worden op artikel 6 lid 1sub f AVG of op één van de grondslagen uit de Wpg. Voor beide interpretaties valt wat te zeggen. Naar het oordeel van Considerati zou het gebruik van spraakherkenning het beste als onderdeel van de politietaak gezien kunnen worden. Dit zorgt er namelijk voor dat de gegevens qua bescherming (autorisaties, bewaartermijnen, verslaglegging et cetera) binnen hetzelfde juridische regime vallen. Het gevolg hiervan is dat de juridisch complexe constructies van overheveling van politiegegevens vanuit de Wpg naar de AVG voorkomen kan worden en de bescherming dus gelijk is.

Een aanvullend argument voor de legitimiteit van de verwerking in de context van de Wpg is dat artikel 4 lid 1 Wpg bepaalt dat politiegegevens juist en volledig moeten zijn en dat de verwerkingsverantwoordelijke daartoe maatregelen moet treffen. Spraakherkenning kan de kwaliteit van de vastlegging van gegevens uit bijvoorbeeld een verhoor vergroten

en zorgen voor een meer volledige weergave van het verhoor. Hiermee draagt spraakherkenning bij aan de doelstelling van artikel 4 lid1 Wpg.

6.2.3 Wjsg

Net zoals de Wpg, bepaalt ook de Wjsg de specifieke voorwaarden waaronder Wjsg-gegevens verwerkt mogen worden. De Wjsg maakt, zoals in paragraaf 4.3.3. is beschreven, onderscheid tussen justitiële gegevens, strafvorderlijke gegevens, persoonsdossiers, tenuitvoerleggingsgegeven en gerechtelijke strafgegevens.

Justitiële gegevens worden door de Minister van Veiligheid en Justitie verwerkt in de justitiële documentatie ten behoeve van een goede rechtspleging (artikel 2 lid 1 Wjsg). Welke gegevens in dit geval als justitiële gegevens kwalificeren wordt bij algemene maatregel van bestuur bepaald (artikel 2 lid 2 Wjsg).

Strafvorderlijke gegevens worden door het College van procureurs-generaal – tevens verwerkingsverantwoordelijke – slechts verwerkt indien dit noodzakelijk is voor een goede vervulling van de taak van het openbaar ministerie of het nakomen van een andere wettelijke verplichting (artikel 39a lid 1 jo. artikel 39b lid 1 Wjsg). Hierbij dient de verwerkingsverantwoordelijke per proces een duidelijk onderscheid te maken tussen verschillende categorieën betrokkenen (artikel 39b lid 2 Wjsg).

Persoonsdossiers worden door de Minister van Veiligheid en Justitie in de documentatie persoonsdossiers verwerkt met het oog op de juiste toepassing van het strafrecht (artikel 40 lid 1 Wjsg).

Tenuitvoerleggingsgegevens worden door de Minister van Veiligheid en Justitie of het College van procureurs-generaal verwerkt indien dit noodzakelijk is voor een goede vervulling van een wettelijke taak of het nakomen van een andere wettelijke verplichting (51a lid 1 Wjsg).

Gerechtelijke strafgegevens worden slechts verwerkt voor zover dit noodzakelijk is voor de rechtspraak (artikel 51e Wjsg).

Indien persoonsgegevens worden verwerkt bij de toepassing van spraakherkenning door de in paragraaf 3.3. beschreven *use case* van een fictieve JenV instantie, moet eerst bepaald worden of er sprake is van een verwerking van Wjsg-gegevens. Indien dit zo is wordt per proces nagegaan op welke grondslag de verwerkingsactiviteit gebaseerd wordt.

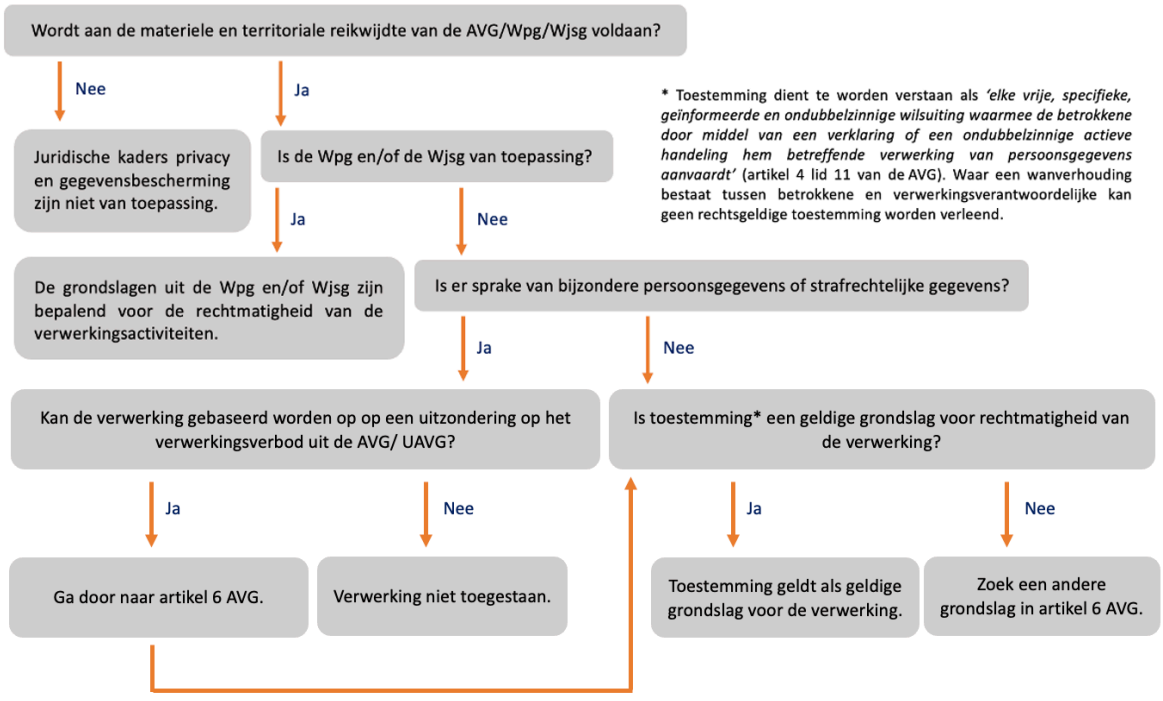
Daarnaast blijkt uit de fictieve *use case* die in paragraaf 3.3. is beschreven, dat spraakherkenning binnen de fictieve JenV instantie in het Wjsg-domein ook wordt toegepast tijdens vergaderingen tussen werknemers onderling. Welk regime op de verwerking van persoonsgegevens hierbij van toepassing is, hangt af van de vraag of er sprake is van de verwerking van Wjsg-gegevens. Indien dit het geval is, is de Wjsg bepalend voor de vaststelling van de legitimiteit van de verwerkingsactiviteiten en de verdere voorwaarden en vereisten die van toepassing zijn. Indien sprake is van de verwerking van persoonsgegevens maar geen Wjsg-gegevens, bijvoorbeeld in het geval van een interne vergadering over bedrijfsvoering en organisatie, is de AVG van toepassing voor wat betreft de voorwaarden en vereisten waar de verwerkingsactiviteiten aan moeten voldoen. Per proces moet dan worden beoordeeld of de verwerking gebaseerd kan worden op artikel 6 lid 1 sub f AVG: het gerechtvaardigd belang. Bij de beoordeling van welk regime op de verwerkingsactiviteiten van de fictieve JenV instantie in het Wjsg-domein van toepassing is, moet worden overwogen wie bij deze vergaderingen betrokken zijn en wat de inhoud van deze vergaderingen is.

Net als bij de Wpg is naar het oordeel van Considerati wenselijk dat die gegevens die worden verwerkt in het kader van de primaire processen van de organisatie (de strafrechtspleging) met behulp van spraakherkenning ook vallen binnen het domein van de Wjsg. Op die manier blijven de gegevens qua bescherming binnen hetzelfde regime. Wanneer spraakherkenning niet direct als onderdeel van het uitvoeren van de taken in het kader van de Wjsg wordt gezien, biedt de verenigbaarheidstoets van artikel 3 lid 6 Wjsg

mogelijk nog uitkomst. Die toets houdt in dat justitiële gegevens voor een ander doel dan waarvoor zij zijn verzameld verwerkt mogen worden indien de verwerking niet onverenigbaar is met het oorspronkelijke verzameldoel. Het is goed verdedigbaar dat het gebruiken van de gegevens ten behoeve van auto-transcriptie verenigbaar is met de doelen die de Wjsg voor ogen heeft. Immers, de gegevens worden verwerkt met als doel om het primaire proces waartoe de gegevens zijn verzameld te verbeteren.

6.2.4 Overzicht mogelijke wettelijke grondslagen

Welke grondslagen van toepassing zijn bij de verwerking van persoonsgegevens in de context van spraakherkenning is dus afhankelijk van het toepassingsdomein. Het onderstaande schema kan gebruikt worden om te bepalen welke grondslagen van toepassing zijn en of rekening moet worden gehouden met uitzonderingsgronden voor het gebruik van strafrechtelijke gegevens, politiegegevens, of bijzondere persoonsgegevens.



Afbeelding 8. Grondslagen toepassing spraakherkenning binnen JenV-domein.

Nota bene:

De verwerking van persoonsgegevens moet altijd gebaseerd worden op een wettelijke grondslag uit één van de toepasselijke juridische kaders (AVG, Wpg of Wjsg). Wij gaan er in dit rapport vanuit dat deze grondslag gelijk is (of zou moeten zijn) aan de juridische grondslag die wordt gebruikt voor het huidige proces voor het vastleggen van gegevens. Bijvoorbeeld: de verwerking van persoonsgegevens binnen een verslag van een verhoor van een verdachte kan gebaseerd worden op artikel 9 Wpg; terwijl de verwerking van persoonsgegevens in een gespreksverslag met een cliënt bij de Reclassering gebaseerd kan worden op artikel 6e AVG (de taak van algemeen belang of openbaar gezag).

Een alternatieve wijze om de verwerking van persoonsgegevens door middel van spraakherkenning te beschouwen is dat de verwerking puur een bedrijfsmatige/facilitaire aangelegenheid is. Hoewel het gebruik van de persoonsgegevens nog steeds gebaseerd moet kunnen worden op één van de grondslagen uit de AVG, Wpg of Wjsg zoals hierboven beschreven, zou de vastlegging ervan dan gebaseerd worden op de gerechtvaardigde belangen van de verwerkingsverantwoordelijke (6f AVG). Het argument is dan dat spraakherkenning noodzakelijk is om de effectiviteit, accuraatheid en efficiëntie van de organisatie te vergroten. In deze rapportage gaan wij uit van de eerste benadering waarbij de grondslag moet worden gezocht in de Wpg of Wjsg, omdat de gegevens dan binnen hetzelfde juridische regime blijven en er dus niet twee aparte juridische kaders (met uiteenlopende bescherming) van toepassing zijn.

6.3 Gegevensopslag

Zoals in eerder in dit rapport is besproken, gelden bij de ontwikkeling en toepassing van spraakherkenning binnen het JenV-domein verschillende wettelijke regimes op het gebied van privacy en gegevensbescherming. Welk regime van toepassing is hangt af van de persoonsgegevens die worden verwerkt en het doel waarvoor deze worden verwerkt. Dit beïnvloedt ook de bewaartermijnen die op de opslag van de betreffende persoonsgegevens van toepassing zijn. In deze paragraaf staan we stil bij de wettelijk geregelde bewaartermijnen die van toepassing zijn op de opslag van persoonsgegevens voor organisaties binnen het JenV-domein waar spraakherkenning wordt toegepast: de AVG, Wpg, Wjsg en Archiefwet.

6.3.1 AVG

Artikel 5 lid 1 sub e AVG bepaalt dat persoonsgegevens in beginsel enkel bewaard mogen worden in een vorm die het mogelijk maakt de betrokkene(n) niet langer te identificeren dan voor de doeleinden waarvoor de verwerking van persoonsgegevens noodzakelijk is. Met andere woorden, persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor het doel van de verwerking. Dit eist op grond van overweging 39 AVG dat ervoor wordt gezorgd dat de opslagperiode van de persoonsgegevens tot een strikt minimum wordt beperkt. Wanneer de gegevens niet langer noodzakelijk zijn, moeten deze worden vernietigd of gewist.

De AVG bepaalt niet wat de specifieke bewaartermijn voor persoonsgegevens is. Het uitgangspunt is dat persoonsgegevens niet langer mogen worden verwerkt dan noodzakelijk is om de doeleinden te bereiken. Organisaties waarop de AVG van toepassing is, zoals de Reclassering bepalen zelf hoe lang het nodig is om persoonsgegevens te bewaren om de voorgenomen doeleinden te bereiken.

In beginsel omvat de AVG dus geen specifieke bewaartermijnen. Wel kan de wetgever, binnen de grenzen van de AVG, verplichte bewaartermijnen opleggen aan verwerkingsverantwoordelijken. In Nederland gaat dit via diverse materiewetten en voor archivering van overheidsbestanden bestaat de archiefwet.

6.3.2 Wpg

De Wpg schrijft vaste bewaartermijnen voor politiegegevens voor. In artikel 4 lid 2 Wpg staat dat de verwerkingsverantwoordelijke de nodige maatregelen treft om te verzekeren dat politiegegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verwerkt of dit door enige wettelijke bepaling wordt vereist. Hieruit blijkt onder meer dat de Wpg een onderscheid maakt tussen het verwijderen en vernietigen van gegevens. De Wpg spreekt van het verwijderen van politiegegevens waar politiegegevens slechts niet langer voor algemeen toegankelijk zijn voor alle politieambtenaren, terwijl zij van *vernietiging van politiegegevens* spreekt waar deze permanent en volledig ontoegankelijk zijn.

Artikel 14 Wpg bepaalt de bewaartermijnen waaraan de politie dient te voldoen bij de verwerking van politiegegevens. Politiegegevens worden gedurende een termijn van vijf jaar bewaard ten behoeve van de verwerking met het oog op de afhandeling van klachten en de verantwoordingen van verrichtingen, waarna deze worden vernietigd overeenkomstig de bepalingen in de Wpg (*zie* tabel1).

Bepaling	**Doel**	**Wettelijke onderbouwing**
Politiegegevens worden vernietigd zodra deze niet langer noodzakelijk zijn voor de uitvoering van de dagelijkse politietaak. Politiegegevens worden in ieder geval uiterlijk vijf jaar na de datum van eerste verwerking verwijderd.	Uitvoering van de dagelijkse politietaak	Artikel 8 lid 6 Wpg
Politiegegevens worden verwijderd wanneer deze niet langer noodzakelijk zijn voor het doel van het onderzoek. *- of –* Politiegegevens worden gedurende een periode van maximaal een half jaar verwerkt teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek (artikel 9 Wpg) of een nieuwe verwerking (artikel 10	Onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval	Artikel 9 lid 4 Wpg

Wpg) en na verloop van deze termijn verwijderd.		
Politiegegevens worden verwijderd zodra zij niet langer noodzakelijk zijn voor het doel van de verwerking en hiertoe worden de gegevens periodiek gecontroleerd. Politiegegevens worden verwijderd uiterlijk vijf jaar na de datum van de laatste verwerking van gegevens die blijk geeft van de noodzaak tot verwerking voor dit doel.	Inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde	Artikel 10 lid 6 Wpg
Politiegegevens worden vernietigd zodra zij niet langer noodzakelijk zijn voor het doel van de verwerking en daartoe worden de gegevens elk halfjaar gecontroleerd. Politiegegevens worden vernietigd uiterlijk 10 jaar na de datum van de laatste verwerking van gegevens die blijk geeft van de noodzaak tot het verwerken van politiegegevens voor dit doel.	Informanten	Artikel 12 lid 6 Wpg

Tabel 1. *Termijnen voor vernietiging en verwijdering politiegegevens o.g.v. de Wpg.*

Tot slot staat in artikel 14 lid 3 Wpg dat politiegegevens die in overeenstemming met de Wpg worden bewaard, voor zover dat noodzakelijk is voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (artikel 9 Wpg) of ten behoeve van het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (artikel 10 Wpg) in opdracht van het bevoegd gezag (op grond van de Politiewet 2012) ter beschikking kunnen worden gesteld voor hernieuwde verwerking.

Gelet op het bovenstaande geldt voor de politie dat zij zich voor wat betreft de opslag van politiegegevens in de vorm van audio-opnames en (door spraakherkenning gegenereerde) transcripten in het kader van het verhoor, het digitaal gesproken zakboekje of de meldkamer, aan verschillende bewaartermijnen in de Wpg gebonden is. Daarnaast gelden ten aanzien van de politie ook specifieke bewaartermijnen voor archivering (zie paragraaf 6.3.4.).

6.3.3 Wjsg

De Wjsg schrijft vaste bewaartermijnen voor. Artikel 3 lid 7 Wjsg stelt dat de Minister van Veiligheid en Justitie de nodige maatregelen treft om te verzekeren dat justitiële gegevens worden verwijderd of vernietigd zodra deze niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verwerkt of waar dit door enige wettelijke bepaling wordt vereist. Zo bepaalt artikel 41 Wjsg over rapporten in een personendossier dat deze verwijderd moeten worden na verloop van 10 jaar vanaf de dag van sluiting van het rapport. Daarnaast moeten gerechtelijke strafgegevens worden verwijderd zodra deze voor de gerechten niet langer noodzakelijk zijn voor de uitoefening van hun gerechtelijke taken.

Ook bepaalt artikel 19 Wjsg over het verstrekken van justitiële gegevens dat elke verstrekking wordt vastgelegd en ten minste vier jaar wordt bewaard (artikel 51g Wjsg). Daarnaast wordt in de Wsjg onderscheid gemaakt tussen de bewaartermijnen voor de opslag van justitiële gegevens van verdachten en veroordeelden van misdrijven en de

opslag van justitiële gegevens van verdachten en veroordeelden van overtredingen, zoals hieronder verder uitgewerkt.

Opslag justitiële gegevens verdachten en veroordeelden misdrijven

Ten aanzien van verdachten en veroordeelden wegens misdrijven bepaalt artikel 4 lid 1 Wjsg dat justitiële gegevens die op hen betrekking hebben worden vernietigd:

- 30 jaar nadat een beslissing om niet te vervolgen is genomen:
  - nadat een einduitspraak is gedaan in verband met een misdrijf waarop een gevangenisstraf van (meer dan) zes jaar is gesteld en in het kader van dat misdrijf de justitiële gegevens zijn verwerkt; of
  - nadat een strafbeschikking wegens het misdrijf volledig ten uitvoer is gelegd, dan wel twintig jaar na het overlijden van betrokkene.
- 20 jaar nadat een beslissing om niet te vervolgen is genomen:
  - nadat een einduitspraak is gedaan in verband met een misdrijf waarop een gevangenisstraf van minder dan zes jaar is gesteld en in het kader van het misdrijf de justitiële gegevens zijn verwerkt; of
  - nadat een strafbeschikking wegens het misdrijf volledig ten uitvoer is gelegd, dan wel twaalf jaar na het overlijden van betrokkene.
- Na het vervallen van het recht tot strafvordering door verjaring.

Daarnaast regelt artikel 4 lid 2 Wjsg dat deze termijnen worden verlengd als tegen de betrokkene een einduitspraak is gedaan in verband met een ander misdrijf; in dat geval worden de justitiële gegevens vernietigd twintig dan wel dertig jaar nadat het vonnis is uitgesproken of de strafbeschikking volledig ten uitvoer is gelegd. Ook geldt ten aanzien van de termijn van 30 jaar dat deze met twintig jaar wordt verlengd indien de duur van de gevangenisstraf of vrijheidsbenemende maatregel langer is dan twintig jaar. Indien de gevangenisstraf levenslang is of de vrijheidsbenemende maatregel de duur van veertig jaar overstijgt, worden de justitiële gegevens pas na tachtig jaar vernietigd (artikel 4 lid 3 Wjsg). Als de gevangenisstraf levenslang is of de vrijheidsbenemende maatregel de duur van veertig jaar overstijgt, worden de justitiële gegevens pas na tachtig jaar vernietigd (artikel 4 lid 3 Wjsg). Hetzelfde geldt ten aanzien van justitiële gegevens die betrekking hebben

op verdachten en veroordeelden wegens misdrijven op het gebied van zeden en seksueel misbruik (artikelen 240b-250 Wetboek van Strafrecht) (artikel 4 lid 4 Wjsg).

Opslag justitiële gegevens verdachten en veroordeelden overtredingen

Ten aanzien van verdachten en veroordeelden wegens overtredingen bepaalt artikel 6 Wjsg dat justitiële gegevens die op hen betrekking hebben worden vernietigd:

- 5 jaar nadat een beslissing om niet te vervolgen is genomen:
  - nadat een einduitspraak is gedaan in verband met een overtreding en in het kader van de overtreding de justitiële gegevens zijn verwerkt; of
  - een strafbeschikking wegens een overtreding volledig ten uitvoer is gelegd.
- 10 jaar nadat een beslissing om niet te vervolgen is genomen;
  - nadat een einduitspraak is gedaan in verband met een overtreding en in het kader van de overtreding de justitiële gegevens zijn verwerkt; of
  - een strafbeschikking wegens een overtreding volledig ten uitvoer is gelegd, en daarbij een vrijheidsstraf, vervangende hechtenis daaronder niet begrepen, of een taakstraf is opgelegd, dan wel aan een rechtspersoon een geldboete van de derde categorie of hoger is opgelegd.
- 2 jaar na het overlijden van de betrokken.
- Na het vervallen van het recht tot strafvordering door verjaring.

Zo bezien geldt ten aanzien van instanties binnen het justitiedomein – waaronder ook de instantie die in de fictieve *case study* in paragraaf 3.3. is geïntroduceerd – dat deze voor wat betreft de opslag van wjsg-gegevens in de vorm van audio-opnames en (door spraakherkenning gegenereerde) transcripten aan verschillende bewaartermijnen in de Wjsg gebonden is. Daarnaast gelden ten aanzien van deze instanties ook specifieke bewaartermijnen voor archivering (zie paragraaf 6.3.4.). Uitgangspunt hierbij is dat de toepassing van spraakherkenning binnen het JenV-domein ten aanzien van audio-opnamen en transcripten in principe geen veranderingen teweegbrengt in de regels omtrent bewaartermijnen die normaal gesproken van toepassing zijn. Hierbij wordt wederom een onderscheid gemaakt tussen misdrijven (20 jaar, 30 jaar of verjaring) en overtredingen (2 jaar, 5 jaar, 10 jaar of verjaring).

6.3.4 Archiefwet

Zoals al eerder in dit rapport is aangegeven, kunnen de Archiefwet en eventueel aanvullende selectielijsten een bepalende rol spelen bij de vaststelling van bewaartermijnen voor de opslag van persoonsgegevens door organisaties binnen het JenV-domein. Hoewel het buiten de reikwijdte van dit rapport valt om de precieze regelingen omtrent archivering in kaart te brengen, is het voor dit onderzoek relevant om de specifieke domeinen in de Selectielijst van het Ministerie van Justitie en Veiligheid en rechtsvoorgangers vanaf 5 mei 1945 te benoemen die toezien op:

- Cluster 2: Primaire bedrijfsfuncties. Meer in het bijzonder zijn hierbij de volgende onderwerpen relevant:
    - Opsporing, straf- en rechtsvordering en civielrechtelijke taken;
    - Ten uitvoer leggen strafrechtelijke beslissingen en strafbeschikkingen;
    - Gedragskundig onderzoek en observatie;
    - Ten uitvoer leggen van vrijheidsstraffen en vrijheidsbenemende maatregelen; en
    - Kinderbescherming.
- Cluster 4: ondersteunende functies. Deze categorie is gericht op het ter beschikking stellen van mensen, gebouwen en middelen aan de Rijksdienst zelf ten behoeve van het zo goed mogelijk uitvoeren van de primaire taken. In het kader van de toepassing van spraakherkenning door JenV is deze categorie met name relevant waar het de toepassing van deze technologie tussen medewerkers onderling ten behoeve van de uitvoering van primaire taken betreft (denk bijvoorbeeld aan vergaderingen tussen medewerkers binnen het JenV-domein).

6.3.5 Bewaartermijnen voor metadata

Bij de verwerking van persoonsgegevens ten behoeve van de ontwikkeling en toepassing van spraakherkenning, worden ook metadata verwerkt. Metadata omvatten gegevens die de context, de inhoud en de structuur van informatieobjecten – hier: audio-opnames – beschrijven. Zo omvatten metadata onder meer informatie over locaties, duur, tijdstip en bestandsformaat van audio-opnames. Als zodanig geven metadata context aan audio-opnames die door middel van spraakherkenning worden omgezet in transcripten. Hoewel metadata niet op individueel niveau als persoonsgegeven kwalificeren, kunnen deze

gegevens in combinatie met andere persoonsgegevens gebruikt worden om een individu te identificeren en herleiden.

Een voorbeeld hiervan is de locatie van een audio-opname van een verhoor (bijvoorbeeld 'verhoorkamer 1'), wat op zichzelf geen persoonsgegeven is. Ook kan gedacht worden aan de datum en het tijdstip van een audio-opname van een verhoor (bijvoorbeeld 12 september 2022, 15:00 uur), wat op zichzelf ook geen persoonsgegevens zijn. Wanneer deze gegevens echter worden bezien in combinatie met andere gegevens (bijvoorbeeld een lijst met namen van verdachten en de datum en het tijdstip waarop zij zijn verhoord), dan kunnen de audio-opnamen alsnog aan een bepaalde persoon gekoppeld worden en kunnen daar wellicht bepaalde kenmerkende gegevens uit worden afgeleid (bijvoorbeeld type verhoor).

In combinatie met de audio-opnames kunnen metadata meer context geven aan de informatie die door middel van spraakherkenning wordt omgezet in tekst. Waar spraakherkenning wordt toegepast in het JenV-domein zouden metadata bijvoorbeeld de locatie van opname kunnen weergeven. Wanneer dit een specifieke verhoorkamer van de politie betreft, kunnen deze metadata betekenis toekennen aan de relevante audio-opname(s) en die aanvullende betekenis kan – afhankelijk van de omstandigheden en overige beschikbare persoonsgegevens - gevoelig van aard zijn.

Als algemene regel gelden daarom dat voor metadata dezelfde vereisten en voorwaarden voor bescherming op het gebied van privacy en gegevensbescherming gelden als voor andere categorieën van persoonsgegevens. Wat betreft de bewaartermijnen voor metadata gelden daarom dat de hierboven beschreven regimes voor opslag van toepassing zijn.

6.4 Training van systemen

Het trainen van AI, zoals een spraakherkenningssysteem, omvat diverse verwerkingspraktijken. Het gevolg hiervan is dat de AVG hierop van toepassing is en dat aan de voorwaarden en beginselen hiervan moet worden voldaan. Hoewel het getrainde

spraakherkenningsmodel zelf geen persoonsgegevens bevat, moet het systeem om tot dat model te komen met trainingsdata worden gevoed. De trainingsdata kunnen persoonsgegevens bevatten. Bij het trainen en hertrainen van spraakherkenningsmodellen moet een balans worden gezocht tussen de wens om zoveel mogelijk trainingsdata te gebruiken om het model optimaal te laten presteren en het vereiste van data minimalisatie uit de AVG.[65]

Hierna bespreken we de privacyrechtelijke aspecten van het (her)trainen van spraakherkenningssystemen. Hierbij maken we een onderscheid tussen het (her)gebruik van persoonsgegevens als trainingsdata voor de ontwikkeling van spraakherkenning binnen de in hoofdstuk 3 besproken JenV instanties. Daarnaast werpen we een blik op de voorwaarden en vereisten voor het delen van deze trainingsdata gegenereerd binnen het JenV-domein voor de ontwikkeling van spraakherkenningstechnologie buiten het JenV-domein.

6.4.1 AVG

6.4.1.1 (Her)trainen van spraakherkenning binnen het JenV-domein

Zoals in paragraaf 4.2.2 beschreven is, dient bij het vaststellen van de legitimiteit van een verwerking eerst te worden bepaald of aan de beginselen van doelspecificatie en doelbinding is voldaan (artikel 5 lid 1 sub b AVG). Persoonsgegevens mogen enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en zij mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt.

Wanneer gegevens nieuw worden verzameld dan kan de verwerkingsverantwoordelijke (her)training als één van de doelen van de verwerking definiëren. Deze verwerking moet dan op één van de grondslagen uit artikel 6 AVG kunnen worden gebaseerd. Zowel de publieke taak (6e AVG) als 6f (gerechtvaardigd belang) zouden hiervoor in aanmerking komen. Onderbouwd moet worden dat de verwerking noodzakelijk is voor de

[65] AP (2020). Toezicht op AI & Algoritmes. Geraadpleegd op 5 april 2022, van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezicht_op_ai_en_algoritmes.pdf.

verwerkingsverantwoordelijke en voldoet aan de eisen van proportionaliteit en subsidiariteit.

Wanneer een organisatie uit het justitie- en veiligheidsdomein reeds bestaande gegevens (bijvoorbeeld opgenomen verhoren) wil gebruiken voor het (her)trainen van een spraakherkenningsmodel dan is er mogelijk sprake van een nieuw verwerkingsdoel. Allereerst moet worden vastgesteld of de verwerking past binnen het bestaande verwerkingsdoel en aldus door die grondslag wordt gedekt. Hoewel het zeker niet ondenkbaar is dat dit kan, is het wel moeilijker te betogen dan voor het daadwerkelijk toepassen van spraakherkenning in het primaire proces zoals besproken in paragraaf 6.2, omdat het trainen van een spraakherkenningsmodel en het primaire proces waarin dit model gebruikt gaat worden verder van elkaar staan.

Verenigbaarheid

Wanneer niet volgehouden kan worden dat het (her)trainen een noodzakelijk onderdeel is van de oorspronkelijke verwerking, dan moet worden teruggevallen op het verenigbaarheidscriterium (artikel 6 lid 4 AVG). Of een verdere verwerking verenigbaar is met het oorspronkelijke verzameldoel wordt beoordeeld aan de hand van de verenigbaarheidstoets die bestaat uit de volgende onderdelen:

1. Het verband tussen het oorspronkelijke doel en het nieuwe doel;
2. De context waarin de gegevens zijn verzameld (wat is de relatie tussen verwerkingsverantwoordelijk en betrokkenen?);
3. De soort en aard van de gegevens (betreft het gevoelige of bijzondere persoonsgegevens?);
4. De mogelijke gevolgen van de verdere verwerking (wat zijn de gevolgen voor de betrokkenen?);
5. Het bestaan van passende waarborgen (zoals versleuteling of pseudonimisering).

Het is aan de verwerkingsverantwoordelijke om de weging te maken. Hoewel de verwerkingen niet heel dicht bij het oorspronkelijke doel, biedt het feit dat de impact op

de betrokkene in beginsel miniem is (zeker als daar voldoende waarborgen voor zijn getroffen) aanknopingspunten om te betogen dat de verwerking verenigbaar is.

Wat tenslotte nog relevant is, is dat onder de nieuwe AI Verordening een speciale bepaling gecreëerd is die het mogelijk maakt om voor AI toepassingen met een zwaarwegend algemeen belang af te wijken van het doelbindingscriterium. Deze mogelijk gaat echter alleen bestaan voor partijen die meedoen in zogenaamde 'AI regulatory sandboxes'.

Toelichting: verenigbaar of niet?

Of een nieuw doel verenigbaar is met het oorspronkelijke verzameldoel hangt af van de omstandigheden van het geval. Onderstaand geven wij enkele voorbeelden om de verenigbaarheidstoets wat tastbaarder te maken.

Het verband tussen het oorspronkelijke doel en het nieuwe doel

Hoe sterker het verband tussen het oorspronkelijke doel en het nieuwe doel, hoe eerder de verwerking verenigbaar is. Het gebruik van verhoren voor het trainen van een spraakherkenningsmodel dat gebruikt wordt voor een klantloket is bijvoorbeeld minder snel verenigbaar te achten dan het gebruik van het model voor het verbeteren van de kwaliteit van het verhoor.

Wat ook nog relevant is, is dat het trainen van spraakherkenning voor een bepaalde context het beste werkt met gegevens uit die context (het toepassingsdomein). Dit kan als argument worden meegenomen in de verenigbaarheidstoets: om de verwerking van persoonsgegevens binnen het oorspronkelijke doel te verbeteren, moeten de gegevens voor het secundaire doel worden gebruikt (het trainen van de spraakherkenning).[66]

De context waarin de gegevens zijn verzameld

[66] Zie in dit kader ook: ECLI:EU:C:2022:805.

De gegevens die worden verzameld van betrokkenen in het JenV-domein betreffen doorgaans gegevens van justitiabelen. Het betreft hier gegevens van (kwetsbare) personen waar soms zelfs tegen hun wil gegevens worden verzameld. Dit is een negatieve indicatie voor verenigbaarheid. Of dit het geval is moet aan de hand van de context worden beoordeeld. De context van een verhoor is bijvoorbeeld gevoeliger dan de context van een vergadering.

De soort en aard van de gegevens

Gegevens uit het justitie- en veiligheidsdomein zijn doorgaans gevoelig. Dit hangt echter af van welke (delen) van gesprekken worden geselecteerd voor het trainen. Zo zijn opnamen van een verhoor van een kwetsbare verdachte gevoeliger (en daarmee minder snel verenigbaar) dan opnamen van een gesprek met een getuige van een simpele winkeldiefstal.

De mogelijke gevolgen van de verdere verwerking

Wanneer de verwerking van gegevens in een andere context (grote) gevolgen heeft voor de betrokkene, dan is de verwerking doorgaans niet verenigbaar. Wanneer bijvoorbeeld een supermarkt klantgegevens verkoopt aan een verzekeringsmaatschappij om premies te berekenen is er weinig kans dat deze verwerking verenigbaar is. Bij het gebruik van persoonsgegevens voor het trainen van spraakherkenningsmodellen zijn de gevolgen voor de betrokkene in beginsel miniem. Het spraakherkenningmodel zelf bevat geen persoonsgegevens en de gegevens beïnvloeden verder niet de situatie van de betrokkene. Het primaire risico voor de betrokkene is dat de gegevens lekken bij het (her)trainen van het model.

Het bestaan van passende waarborgen

Er zijn diverse waarborgen die getroffen kunnen (en moeten) worden om te zorgen voor een verenigbare verwerking. Hierbij kan onder andere gedacht worden aan

pseudonimisering, het verwijderen van metadata en de beveiliging van de gegevens. Verder moeten de gegevens worden verwijderd wanneer zij niet meer relevant zijn voor het trainen.

Niet verenigbare verwerking

Mocht de verwerking niet verenigbaar zijn, dan is deze in beginsel niet toegestaan. De AVG bepaalt dat de verdere verwerking voor een ander niet-verenigbaar doel enkel is toegestaan als de verdere verwerking berust op toestemming van de betrokkene(n)[67] of op een Unierechtelijke bepaling of lidstaatrechtelijke bepaling, dat een noodzakelijke en evenredige maatregel is in een democratische samenleving ter waarborging van een belangrijke doelstelling van algemeen belang, bijvoorbeeld de nationale veiligheid, de openbare veiligheid, monetaire, budgettaire of fiscale aangelegenheden.

Nota bene: statistische doeleinden

Wanneer gegevens voor 'statistische doeleinden' worden gebruikt, dan wordt op grond van artikel 5 jo artikel 89 AVG een dergelijke verwerking op voorhand als verenigbaar gezien. Wel vereist artikel 89 lid 1 AVG dat een dergelijke verwerking is onderworpen aan passende waarborgen in overeenstemming met het overige bepaalde in de AVG ten aanzien van de rechten en vrijheden van de betrokkene die er zorg voor dragen dat er technische en organisatorische maatregelen zijn getroffen om het beginsel van minimale gegevensverwerking te garanderen.

Machine learning maakt gebruikt van statistische methoden om tot resultaten te komen. Dit is evenwel niet hetzelfde als een statistisch doel. Wat echter precies bedoeld wordt met de bewoordingen *statistische doeleinden* in de zin van artikel 89 lid 1 AVG is niet eenduidig. Hoewel de toepassing van deze uitzonderingsgrond op het trainen van spraakherkenningstechnologie niet kan worden uitgesloten, lijkt het in de context van

[67] Ook hierbij geldt, zoals in paragraaf 6.2.1. is besproken, wordt toestemming niet geldig geacht als grondslag voor de verwerking van persoonsgegevens waar deze toestemming wordt gevraagd in een overheid-burger context. In een dergelijk geval bestaat er namelijk een wanverhouding tussen beiden, met als gevolg dat de betrokkene niet vrijelijk toestemming gegeven kan hebben.

spraakherkenning vooralsnog veiliger om de volledige verenigbaarheidstoets te doorlopen.

6.4.1.2 Delen van trainingsdata voor de ontwikkeling van spraakherkenning

Conform artikel 4 sub 2 AVG, kunnen 'het verstrekken' en 'het ter beschikking stellen' van persoonsgegevens als een verwerking van persoonsgegevens worden gekwalificeerd. In de praktijk betekent dit dat deze activiteiten dienen te voldoen aan de voorwaarden en vereisten uit de AVG, waaronder doelbinding, legitimiteit en zorgvuldigheid (zie hiervoor ook paragraaf 4.2). In het kader van dit rapport, zou dit bijvoorbeeld kunnen betekenen dat de Reclassering – die voor wat betreft de ontwikkeling en toepassing van spraakherkenning, valt onder de reikwijdte van de AVG – haar trainingsdata deelt met instanties binnen en buiten het JenV-domein voor de ontwikkeling van spraakherkenningsmodellen.

Voor een dergelijke verstrekking gaat dezelfde redenering op als hierboven beschreven: de verstrekking moet of: 1) gelezen kunnen worden als onderdeel van de oorspronkelijke verwerking, of 2) verenigbaar zijn met het oorspronkelijke verwerkingsdoel, of 3) gebaseerd zijn op een specifieke wettelijke regeling dan wel toestemming.

Met betrekking tot de verenigbaarheidstoets moet nog in het bijzonder worden meegenomen dat de gegevens aan één of meer derden worden verstrekt. Dit is doorgaans een contra-indicatie voor verenigbaarheid. Maar ook hier geldt: stevige waarborgen verkleinen de risico's en vormen een argument om te betogen dat er sprake is van verenigbaarheid.

Het verdient bovendien opmerking dat het delen van gegevens ten behoeve van het trainen van spraakherkenningsmodellen of het samenwerken aan spraakherkenningsmodellen heeft voor zover Considerati dit kan beoordelen geen invloed op de onafhankelijke positie van OM of Rechtspraak.

6.4.2 Wpg

6.4.2.1 (Her)trainen van spraakherkenning binnen het JenV-domein

Gegevens worden door de politie verwerkt ter uitvoering van de politietaak (artikel 3 Politiewet). Voor de uitvoering van de dagelijkse politietaak biedt artikel 8 Wpg de grondslag. De Memorie van Toelichting bij de Wpg zegt daarover:

De uitvoering van de dagelijkse politietaak wordt wel de oog en oor functie van de politie genoemd. Het gaat hier om het zogenaamde basispolitiewerk. Deze functie omvat alle in artikel 2 van de Politiewet 1993 genoemde onderdelen van de politietaak in een soort eerste lijn-variant. Het basispolitiewerk bestaat uit surveillance, advisering over preventie, afhandeling van de verkeersproblematiek, eenvoudig recherchewerk, verlenen van hulp en handhaven van wetten en regels.

Om deze taak goed uit te voeren moet de politie persoonsgegevens (politiegegevens) verwerken. De redactie van het artikel en de toelichting in de Wpg lijken te impliceren dat de genoemde gegevens altijd direct aangewend worden om de politietaak uit te voeren.

Doorgaans is dit natuurlijk ook zo, maar bij het (her)trainen van spraakherkenningsmodellen worden politiegegevens op een meer indirecte wijze aangewend voor de uitvoering van de politietaak. Ze worden gebruikt om in de toekomst de politietaak eenvoudiger, efficiënter en effectiever te maken. De vraag is in hoeverre de Wpg deze ruimte biedt.[68] Het antwoord op deze vraag is van belang, omdat de Wpg in tegenstelling tot de AVG geen verenigbaarheidstoets kent. Met andere woorden: wanneer een verwerking niet binnen de politietaken past, is deze niet toegestaan op grond van de Wpg. Wel bepaalt de Wpg in artikel 3 lid 3 dat politiegegevens die zijn verkregen voor een in deze wet omgeschreven doel kunnen worden verwerkt voor een ander in deze wet omschreven doel voor zover de Wpg of Unierecht daar uitdrukkelijk in voorziet en de verwerking voor dat andere doel noodzakelijk is en in verhouding staat tot dat doel. Waar

[68] De politie mag verder gegevens verwerken voor ondersteunende taken (artikel 13 Wpg). De in dit artikel genoemde taken zijn echter allemaal direct gerelateerd aan de uitvoering van de politietaken zoals omschreven in de artikelen 8 tot en met 10 Wpg.

de verwerking van politiegegevens aldus geschaard kan worden onder de politietaak, wordt aan deze voorwaarden voldaan.

Wanneer de conclusie echter is dat de politietaak zelf dit soort activiteiten niet omvat, dan moeten we terugvallen op het regime van de AVG. De politie moet dan de gegevens uit het Wpg-regime overhevelen naar het AVG-regime. Artikel 6f AVG (gerechtvaardigd belang) zou dan een mogelijke grondslag bieden. Overigens moet hierbij wel worden aangetekend dat dit overhevelen tussen het regime van de WPG en de AVG geen duidelijke regeling lijkt te kennen. De politie kan op grond van artikel 16 tot en met 24 AVG politiegegevens verstrekken aan derden, maar een 'interne verstrekking' lijkt niet expliciet geregeld. Artikel 15 Wpg biedt weliswaar de mogelijkheid om politiegegevens ter beschikking te stellen aan personen binnen de politie in zoverre zij die nodig hebben voor hun taak en daartoe zijn geautoriseerd. Maar dit geldt wederom alleen voor de politietaak (waardoor gegevens binnen het Wpg regime blijven).

Hierbij moet worden aangetekend dat de wetgever de uitwisseling van gegevens tussen het AVG en het Wpg-regime in beginsel niet afkeurt. In tegendeel, de wetgever stelt in de Memorie van Toelichting:

"Dit betekent overigens geenszins dat de uitwisseling tussen de gegevens die onder de twee verschillende privacyregimes worden verwerkt is uitgesloten. Mede met het oog op de toegenomen behoeften tot gegevensuitwisseling worden in dit wetsvoorstel de mogelijkheden om politiegegevens te verstrekken voor andere doeleinden vergaand verruimd."

De Wpg, het Besluit politiegegevens en de AVG bieden geen eenduidig antwoord op de vraag of het trainen van spraakherkenningsmodellen mogelijk is op grond van artikel 8 Wpg, of dat het intern overhevelen tussen regimes voor dit doel is toegestaan.

Naar onze smaak zou het trainen van spraakherkenningsmodellen binnen de politietaak moeten kunnen vallen. Het eerste argument hiervoor is dat de verwerking ten dienste staat van de uitvoering van de politietaak en dat (her)gebruik van politiegegevens voor het (her)trainen van een spraakherkenningsmodel bijdraagt aan een effectieve uitvoering van de politietaak en ter verbetering van de kwaliteit en juistheid van de politiegegevens (artikel 4 lid 1 Wpg).

Het tweede argument is dat de privacyinbreuk beperkt is, omdat de gegevens enkel worden gebruikt om een model te trainen. Als zodanig is er geen grote impact op de persoonlijke levenssfeer en/of de rechten en vrijheden betrokkenen. Wanneer de gegevens buiten de politie worden gebracht wordt dit argument natuurlijk minder sterk.

Gezien de toegenomen erkenning van de waarde van AI-technologie, waaronder spraakherkenning, binnen het JenV-domein, en de toenemende noodzaak om AI-modellen te trainen met data afkomstig uit het justitiedomein, bevelen wij de wetgever aan hier in wettelijke zin meer duidelijkheid over te scheppen. Dit kan bijvoorbeeld worden meegenomen in het wijzigingstraject van de Wpg.

6.4.2.2 Delen van trainingsdata voor de ontwikkeling van spraakherkenning

Zoals wij in paragraaf 4.3.2.2. bespraken, kent de Wpg een gesloten regime voor de verstrekking en terbeschikkingstelling van politiegegevens (artikelen 15-24 Wpg). Dit betekent in de praktijk voor de politie dat zij slechts onder beperkte voorwaarden politiegegevens mogen delen (structureel dan wel incidenteel) met andere partijen, waaronder ook derden. Bovendien geldt hierbij dat de persoon aan wie politiegegevens zijn verstrekt in beginsel verplicht is tot geheimhouding daarvan (artikel 7 Wpg).

Dit alles brengt met zich mee dat per proces moet worden bepaald of de politie trainingsdata (politiegegevens) mag delen voor het (her)trainen van spraakherkenningssystemen. Hierbij geldt als uitgangpunt dat de politie alleen politiegegevens mag verstrekken/ ter beschikking mag stellen indien dit door de Wpg en/of het Besluit politiegegevens wordt geregeld.

6.4.3 Wjsg

6.4.3.1 (Her)trainen van spraakherkenning binnen het JenV-domein

In het kader van dit rapport, valt de in paragraaf 3.3. besproken *use case* binnen de reikwijdte van de Wjsg, namelijk de fictieve instantie binnen het justitiedomein. Uit deze *use case* blijkt dat deze instantie niet zelf een spraakherkenningssysteem ontwikkelt, maar gebruik maakt van de spraakherkenningstechnologie van een commerciële leverancier. Het spraakherkenningsmodel dat hierbij wordt gebruikt is door deze leverancier ontwikkeld zonder dat hiertoe Wjsg-gegevens zijn verwerkt, tenzij de leverancier het mogelijk maakt voor organisaties om het model nader te specificeren door deze verder te trainen met data die aan die organisatie eigen is. Zoals we in paragraaf 3.3. hebben aangegeven, dient Microsoft Azure ter illustratie van een mogelijk commerciële leverancier van spraakherkenningstechnologie die deze mogelijkheid biedt.

Voorbeeld:

Microsoft Azure is een commerciële leverancier van software voor spraakherkenning en cloudtechnologie. Het model voor spraakherkenning dat in dit voorbeeld wordt gebruikt is door Microsoft getraind zonder dat hiervoor Wjsg-gegevens zijn verwerkt. Aangezien het basismodel voor instanties binnen het Wjsg-domein waarschijnlijk in organisatie-specifieke gevallen niet voldoende aansluit bij het gebruikte vakjargon, is het voor de organisaties die van deze Microsoft dienst gebruik maken mogelijk om dit basismodel aan te passen door het verder te trainen met trainingsdata afkomstig uit het Wjsg-domein (ook wel bekend als *Custom Speech*).

Indien de fictieve instantie binnen het justitiedomein gebruik maakt van het basismodel voor spraakherkenning dat door de commerciële leverancier is getraind, is het aan de leverancier, als verwerkingsverantwoordelijke, om te bepalen en aan te tonen dat de verwerking van persoonsgegevens voor het trainen van het model rechtmatig is. De fictieve instantie moet aantonen dat haar gebruik van het spraakherkenningsmodel legitiem is.

Indien het basismodel echter door de fictieve instantie binnen het justitiedomein wordt aangepast door het model verder te trainen aan de hand van Wjsg-gegevens, geldt dat deze activiteit als een verwerking wordt aangemerkt (artikel 1 sub m Wjsg) en hiervoor moet een passende wettelijke basis bestaan.

Wanneer Wjsg-gegevens worden verwerkt met het oog op het (her)trainen van spraakherkenningssystemen, kunnen twee wettelijke routes bewandeld worden. De Wjsg gaat over de verwerking van persoonsgegevens (Wjsg-gegevens) binnen de strafrechtspleging. Doorgaans is dit natuurlijk ook het geval, maar bij het (her)trainen van spraakherkenningsmodellen worden deze gegevens op een meer indirecte wijze aangewend voor dit doel. Ze worden gebruikt om in de toekomst de werkzaamheden van justitie eenvoudiger, efficiënter en effectiever te maken. De vraag is in hoeverre de Wjsg deze ruimte biedt. Net zoals de AVG kent de Wjsg een verenigbaarheidstoets in artikel 3 lid 6 Wjsg, althans ten aanzien van justitiële gegevens. Deze bepaalt dat justitiële gegevens uitsluitend mogen worden verwerkt voor een ander doel dan waarvoor zij zijn verzameld indien dit doel niet onverenigbaar is met het oorspronkelijke verzameldoel. Ook moet de verwerking voor het tweede doel noodzakelijk zijn en in verhouding staan tot dat doel. Daarnaast geldt dat de verdere verwerking alleen mogelijk is door personen en instanties die bij of krachtens de wet met het oog op een zwaarwegend belang zijn aangewezen. Indien deze route bewandeld wordt, moet per proces en per type Wjsg-gegeven worden aangetoond dat de verdere verwerking van Wjsg-gegevens met het oog op het (her)trainen van de modellen voor spraakherkenning aan deze verenigbaarheidstoets voldoet. Overigens is de Wjsg, onduidelijk over de toepasselijkheid van deze verenigbaarheidstoets op de overige Wjsg-gegevens (niet zijnde justitiële gegevens).

Een tweede mogelijkheid is dat de verwerking van persoonsgegevens door de fictieve instantie binnen het justitiedomein met het oog op het (her)trainen van modellen voor spraakherkenning niet valt binnen de reikwijdte van de Wjsg. Het gaat dan namelijk niet langer om verwerkingen ten behoeve van (een goede) strafrechtspleging. In dat geval zou de AVG een alternatief juridisch kader bieden. Zoals in paragraaf 6.4.2.1. is beschreven,

moet de betreffende fictieve instantie binnen het justitiedomein in dat geval de gegevens uit het Wjsg-regime overhevelen naar het AVG regime. Artikel 6f AVG (gerechtvaardigd belang) biedt dan een mogelijke grondslag. Overigens moet ook hierbij worden aangetekend dat dit overhevelen tussen het regime van de Wjsg en de AVG geen duidelijke regeling lijkt te kennen. Zo bepalen de Wjsg en de Aanwijzing Wet justitiële en strafvorderlijke gegevens bijvoorbeeld ten aanzien van strafvorderlijke gegevens onder welke voorwaarden deze voor buiten de strafrechtspleging gelegen doeleinden mogen worden verstrekt. Dit is enkel mogelijk als het past binnen de taakuitoefening van het Openbaar Ministerie en voor zover dit noodzakelijk is wegens een zwaarwegend algemeen belang. Dat betekent dat strafvorderlijke gegevens niet mogen worden verstrekt op grond van het enkele belang dat de derde daarbij heeft. Daarnaast wordt hierbij ook bepaald dat justitiële gegevens in principe onder dezelfde voorwaarden aan derden kunnen worden verstrekt. Hierbij moet telkens worden nagegaan of de verstrekking van justitiële gegevens (mede) aangewezen is. Hoewel Wjsg aldus bepaalt onder welke voorwaarden (bepaalde) Wjsg-gegevens kunnen worden verstrekt, lijkt een 'interne verstrekking' ten behoeve van taken die niet direct aan strafrechtspleging zijn verbonden en ten aanzien van Wjsg-gegevens in zijn algemeenheid, niet expliciet te worden geregeld.

De Wjsg, het Besluit justitiële en strafvorderlijke gegevens, de Aanwijzing Wet justitiële en strafvorderlijke gegevens en de AVG bieden geen eenduidig antwoord op de vraag of het trainen van spraakherkenningsmodellen mogelijk is op grond van de Wjsg, of dat het intern overhevelen tussen regimes met het oog op het (her)trainen van modellen voor spraakherkenning binnen het Wjsg-domein is toegestaan. Net zoals wij hebben beargumenteerd ten aanzien van de Wpg, zou het (her)trainen van spraakherkenningsmodellen naar onze smaak binnen de Wjsg moeten kunnen vallen. Het eerste argument hiervoor is dat de verwerking ten dienste staat van de uitvoering van een goede strafrechtspleging. Het tweede argument is dat de privacy-inbreuk beperkt is, omdat de gegevens enkel worden gebruikt om een model (verder) te trainen. Als zodanig is er geen grote impact op de persoonlijke levenssfeer en/of de rechten en vrijheden betrokkenen.

Zoals al ten aanzien van de Wpg is aangegeven in paragraaf 6.4.2., is het aan te bevelen dat de wetgever of toezichthouder meer duidelijkheid schept over het intern (her)gebruiken van gegevens en de mogelijke 'sfeerovergang' tussen Wsjg en AVG.

6.4.3.2 Delen van trainingsdata voor de ontwikkeling van spraakherkenning

Zoals wij in paragraaf 4.3.3.2. bespraken, kent de Wjsg een gesloten regime voor de verstrekking en terbeschikkingstelling van Wjsg-gegevens. Dit betekent in de praktijk dat Wjsg-gegevens uitsluitend mogen worden verstrekt aan derden wanneer dit mogelijk is op grond van een wettelijke bepaling in de Wjsg.

Zo bepaalt de Wjsg onder meer dat het OM strafvorderlijke gegevens kan delen met samenwerkingsverbanden en met andere derden voor buiten de strafrechtspleging gelegen doelen. De Aanwijzing wet Justitiële en strafvorderlijke gegevens bepaalt wanneer en aan wie het OM dit mag doen. Daarbij geldt dat de partijen die deze gegevens ontvangen bij de verdere verwerking hiervan in principe gehouden zijn aan de AVG en de UAVG.

Tot slot bepaalt de Wjsg in artikel 52 dat eenieder die krachtens deze wet de beschikking krijgt over gegevens met betrekking tot een derde, in beginsel verplicht is tot geheimhouding daarvan, tenzij het noodzakelijk is deze gegevens ter kennis te brengen van anderen.

Dit alles brengt met zich mee dat telkens moet worden bepaald of de betreffende fictieve instantie binnen het justitiedomein trainingsdata (Wjsg-gegevens) mag delen voor het (her)trainen van spraakherkenningssystemen. Hierbij geldt als uitgangpunt dat zij alleen Wjsg-gegevens mag verstrekken/ ter beschikking mag stellen indien dit door de Wjsg of een daarop aansluitend besluit wordt geregeld.

6.5 Afname uit de markt en samenwerking met bedrijven

In de voorgaande paragraaf bespraken we welke vereisten de juridische kaders stellen aan het trainen van een spraakherkenningssysteem. Een andere vraag die in dit kader

interessant is, is of en in hoeverre gebruik mag worden gemaakt van data van derde partijen voor het ontwikkelen van modellen voor spraakherkenning binnen het JenV-domein.

De politie ontwikkelt momenteel een 'eigen' spraakherkenningsmodel. Zoals wij in hoofdstuk 3.3. van dit rapport echter bespraken, is het de vraag in hoeverre dit model gebruikt kan worden door andere organisaties binnen het JenV-domein. Mogelijk komt het taalmodel onvoldoende overeen vanwege de verschillen in jargon. Het is daarom interessant om te onderzoeken of organisaties binnen het JenV-domein gebruik kunnen maken van spraakherkenningssoftware van commerciële leveranciers en hoe deze software op een juridisch verantwoorde manier ingezet kan worden. In navolgende paragrafen zoomen wij in op deze vragen.

6.5.1 Bijeenbrengen trainingsdata van verschillende partijen

Binnen Nederland wordt op het gebied van spraakherkenning en autotranscriptie samengewerkt tussen bedrijven, overheden, semipublieke instellingen en kennisinstellingen om deze technologie voor de Nederlandse taal verder te ontwikkelen. Een belangrijk onderdeel hiervan is het 'bijeenbrengen' van trainingsdata van verschillende bovengenoemde partijen. De vraag is hoe dit op een juridisch verantwoorde wijze kan.

Indien de trainingsdata persoonsgegevens bevatten moet er allereerst een grondslag zijn voor het delen van persoonsgegevens tussen partijen. De grondslag is afhankelijk van het juridische regime dat van toepassing is op de organisatie die de gegevens deelt (AVG/Wpg/Wjsg). Omdat de gegevens doorgaans voor andere doelen zullen zijn verzameld moet het delen daarnaast verenigbaar zijn met het oorspronkelijke verwerkingsdoel.

Wanneer de verstrekkers van de trainingsdata buiten het JenV-domein een grondslag hebben voor de verwerking dan kunnen JenV-organisaties deze grondslag hanteren. Omgekeerd geldt hetzelfde: wanneer JenV-organisaties een grondslag hebben voor het

delen, dan mogen organisaties buiten het JenV-domein deze gegevens gebruiken voor het trainen van modellen.

Hierbij is het wel van belang te vermelden dat de JenV context doorgaans zeer gevoelig is en er geen toestemming kan worden gevraagd aan de betrokkenen. Het is ook onwaarschijnlijk dat het verstrekken aan een grote groep publieke en private partijen verenigbaar is met de oorspronkelijke verwerkingsdoelen (zelfs wanneer onderbouwd kan worden dat dit voor wetenschappelijke doeleinden is). Zolang de gegevens niet geanonimiseerd kunnen worden moet zéér terughoudend worden omgesprongen met het delen van trainingsdata met derden, zeker met derden buiten de justitieketen.

6.5.2 Gebruik van spraakherkenningssoftware

Hoewel JenV organisaties zelf spraakherkenningsmodellen kunnen ontwikkelen is het ook interessant om te kijken in hoeverre gebruik kan worden gemaakt van spraakherkenningssoftware van commerciële aanbieders. In paragraaf 3.3. zijn ter illustratie de spraakherkenningssoftware en clouddiensten van Microsoft genoemd, maar deze diensten kunnen ook van andere commerciële leveranciers worden afgenomen.

6.5.2.1 Rijksbreed cloudbeleid

Wanneer een commerciële aanbieder wordt gebruikt, dan zal deze doorgaans haar infrastructuur (opslag en verwerking) en/of spraakherkenningsmodellen aanbieden. Deze diensten kunnen zich 'in de cloud' bevinden.

Eind augustus 2022 is een nieuw Rijksbreed cloudbeleid gepubliceerd waarin een visie op het gebruik van publieke clouddiensten is uitgewerkt. [69] In dit beleid wordt beschreven wanneer overheidsorganisaties gebruik mogen maken van publieke cloudiensten. Onder het nieuwe cloudbeleid mogen overheidsdiensten in beginsel gebruikmaken van publieke clouddiensten. Op de basisregel zijn enkele voorwaarden en uitzonderingen van toepassing.

[69] Link naar het Rijksbrede cloudbeleid.

Zo geldt dat wanneer er persoonsgegevens worden verwerkt in publieke clouddiensten een pre-scan gegevensbeschermingseffectbeoordeling (ook wel: "pre-scan DPIA") moet worden uitgevoerd. Bij een hoog risico moet vervolgens ook een uitgebreide Data Protection Impact Assessment (hierna: "DPIA") uitgevoerd worden. Op basis van de risico's die volgen uit de DPIA kan de betreffende minister voor tot en met departementaal vertrouwelijke informatie beslissen om de publieke clouddienst te gebruiken.

Op basis van het Rijksbrede cloudbeleid is het uitdrukkelijk niet toegestaan om clouddiensten te gebruiken voor staatsgeheim gerubriceerde informatie. Bovendien valt het Ministerie van Defensie buiten scope van het beleid. Samengevat gelden de volgende voorwaarden voor het gebruik van publieke clouddiensten:

Vereiste	**Toelichting**
Departementaal beleid	Alle departementen formuleren hun eigen cloudbeleid en cloudstrategie.
Risicoafweging	Het uitvoeren van een Pre DPIA (en een DPIA bij een hoog risico) is verplicht.
Gekend gebruik	Departementen zijn verplicht om een rapport bij te houden van het gebruik van de publieke cloud en risico's hiervan.
Exit strategie	Er dient een exit strategie opgenomen te worden in de overeenkomst met de leverancier van de openbare clouddienst.
Voldoen aan eisen voor ICT-dienstverlening	Alle typen clouddienstverlening moeten voldoen aan de bestaande voorwaarden voor ICT-dienstverlening.
Toegespitste risicoanalyse	Analyse op de risico's die vanwege marktconcentratie en politieke en geografische spreiding van toepassing zijn.

Cyberveiligheid	Leveranciers of diensten uit landen met een actief cyberprogramma worden uitgesloten.
Openbaarheid	Vanwege de Wet Open Openheid wordt moeten de DPIA's openbaar worden gemaakt.
Opslag en openbaarmaking	Alle opslag en verwerking vindt plaats conform de AVG. Verwerking vindt plaats binnen de EER, of in landen waarvoor een adequaatheidsbesluit voor bestaat op basis van en passend doorgeefmechanisme.[70]
Bijzondere persoonsgegevens	Bij een verwerking van bijzondere persoonsgegevens wordt in principe geen gebruik gemaakt van publieke clouddiensten, tenzij opslag en verwerking aantoonbaar binnen de EER plaatsvindt of voor dit land een adequaatheidsbesluit bestaat.
Basis registraties	In geval van opslag en verwerking van een basisregistratie wordt in principe geen gebruik gemaakt van publieke cloudvoorzieningen.

Tabel 2. Overzicht voorwaarden voor het gebruik van publieke clouddiensten.

6.5.2.2 Overige voorwaarden

Verwerkersovereenkomst
Indien een commerciële leverancier als verwerker dient voor de verwerkingsactiviteiten van de in paragraaf 3.3. beschreven fictieve instantie binnen het justitiedomein, moet op grond van artikel 28 lid 3 AVG tussen beide een verwerkersovereenkomst gesloten moeten worden. Deze overeenkomst bindt de verwerkingsverantwoordelijke en verwerker en bepaalt het onderwerp en de duur van de verwerking, de aard en het doel van de

[70] Indien hier niet aan wordt voldaan dan wordt voor die verwerking en de daarbij horende subverwerkingen de uitgevoerde pre-DPIA of DPIA toegezonden aan CIO Rijk.

verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven.

De AVG bepaalt verder dat wanneer een verwerkingsverantwoordelijke alleen beroep doet op verwerkers die voldoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen om de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene te waarborgen (28 lid 1 AVG). In het kader van dit rapport betekent dit dat een eventuele commerciële leverancier voldoende garanties moet kunnen bieden dat de rechten van betrokkenen worden beschermd waar zij persoonsgegevens verwerkt voor de ontwikkeling en toepassing van spraakherkenning binnen het JenV-domein. Met name de beveiligingsmaatregelen die zij hierbij moet treffen (artikel 28 lid 3 sub c AVG), zullen wij hierna bespreken.

Beveiligingsmaatregelen

De AVG verplicht de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen te treffen om een beschermingsniveau te waarborgen dat is afgestemd op het risico dat gepaard gaat met de verwerkingsactiviteiten (artikel 32 lid 1 AVG). Hierbij wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten alsook de aard, de omvang, de context en het verwerkingsdoel en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen.

In de verwerkersovereenkomst tussen verwerkingsverantwoordelijke en verwerker wordt onder meer bepaald dat alle overeenkomstig artikel 32 AVG vereiste beveiligingsmaatregelen moet nemen. Deze omvatten onder meer:

- de pseudonimisering en versleuteling van persoonsgegevens;
- de mogelijkheid om de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten op permanente basis te garanderen;

- de capaciteit om ingeval van een technisch of fysiek incident de beschikbaarheid van en toegang tot persoonsgegevens tijdig te herstellen; en
- het beschikken over een procedure aan de hand waarvan op gezette tijdstippen de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerkingsactiviteiten kan worden getest, beoordeeld en geëvalueerd.

In het kader van dit rapport betekent dit dat een eventuele commerciële leverancier ertoe gehouden is passende technische en organisatorische maatregelen te treffen om de risico's die de verwerking van persoonsgegevens voor de ontwikkeling en toepassing van spraakherkenning binnen het JenV-domein met zich meebrengen te beperken.

Tot slot bepaalt artikel 32 lid 4 AVG dat de verwerkingsverantwoordelijke en de verwerker maatregelen moeten treffen om ervoor te zorgen dat persoonsgegevens slechts worden verwerkt in opdracht van de verwerkingsverantwoordelijke.

Zoals hierboven beschreven, bieden sommige commerciële leveranciers, waaronder Microsoft, de mogelijkheid om de door hen ontwikkelde taalmodellen verder te trainen zodat zij aansluiten op de specifieke taalmodellen die de afnemers van hun diensten nodig hebben. Met het oog op doelbinding en minimale gegevensverwerking, is het van belang duidelijke afspraken te maken met de betreffende commerciële leverancier over de grenzen waarbinnen persoonsgegevens afkomstig uit het JenV-domein verwerkt mogen worden. Zo brengt dit bijvoorbeeld met zich mee dat met de betreffende commerciële leverancier overeengekomen moet worden dat trainingsdata vanuit het JenV-domein niet verwerkt worden voor eigen doeleinden (waaronder het trainen van het model voor de eigen bredere commerciële toepassing).

Doorgifte van persoonsgegevens

Verder geldt dat bij de afname van spraakherkenningstechnologie van commerciële leveranciers sprake mogelijk sprake is van doorgifte van persoonsgegeven buiten de EER. Hieronder wordt ook toegang tot persoonsgegevens vanuit een derde land verstaan.

Voorbeeld

Omdat Microsoft een Amerikaanse partij is vindt bij gebruik van de spraakherkenningssoftware van Microsoft mogelijk doorgifte van persoonsgegevens plaats. Hiermee wordt doorgaans bedoeld het ter kennis brengen van persoonsgegevens aan een ontvanger in een land buiten de EER (derde land). Ook toegang tot persoonsgegevens vanuit een derde land valt onder deze definitie.

AVG

De AVG stelt strikte voorwaarden aan doorgiften persoonsgegevens. Het doel hiervan is om te voorkomen dat het beschermingsniveau wordt ondermijnd wanneer dit in een derde land minder hoog is.

Artikel 44 AVG regelt dat persoonsgegevens enkel mogen worden doorgegeven indien is voldaan aan de voorwaarden artikelen 44 t/m 50 in de AVG. In deze artikelen staan verschillende instrumenten die gebruikt kunnen worden om de doorgifte te laten plaatsvinden.

De AVG maakt vrije doorgifte allereerst mogelijk indien de Europese Commissie in een adequaatheidsbesluit besluit dat een derde land, gebied of sector in een derde land een passend beschermingsniveau waarborgt (artikel 45 AVG).

Wanneer een dergelijk adequaatheidsbesluit ontbreekt mag een verwerkingsverantwoordelijke of verwerker enkel persoonsgegevens doorgeven indien

passende waarborgen worden geboden in de vorm van instrumenten zoals goedgekeurde bindende bedrijfsvoorwaarden (BCR's), goedgekeurde gedragscodes of certificeringsmechanismen en modelcontractbepalingen (SCCs) van de Europese Commissie.

Wanneer een adequaatheidsbesluit ontbreekt en ook niet een van de passende waarborgen van toepassing is, kan doorgifte alleen plaatsvinden indien een van de specifieke situaties uit artikel 49 AVG van toepassing is. Bijvoorbeeld wanneer de doorgifte noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke (artikel 49 lid 1 sub b).

Wpg en Wjsg

Artikel 17a Wpg regelt doorgifte van politiegegevens naar derde landen. Politiegegevens kunnen worden doorgegeven aan een derde land of internationale organisatie als dit noodzakelijk is voor het uitvoeren van de politietaak. Wjsg-gegevens kunnen op basis van artikel 16a Wjsg worden doorgegeven indien dit noodzakelijk is ten behoeve van de strafrechtspleging. Bovendien geldt voor zowel politiegegevens als Wjsg-gegevens als aanvullend vereiste dat de Europese Commissie heeft besloten dat het derde land een passend beschermingsniveau heeft. Als dit ontbreekt mogen politiegegevens/Wjsg-gegevens worden doorgegeven indien:

- In een juridisch bindend instrument passende waarborgen worden geboden; of
- De verwerkingsverantwoordelijke op basis van een beoordeling van de omstandigheden van het geval beoordeeld dat passende waarborgen worden genomen voor de bescherming van persoonsgegevens en de Autoriteit Persoonsgegevens wordt geïnformeerd.

Cloudbeleid

Het Rijksbrede Cloudbeleid dat wij in paragraaf 6.5.2.1 van dit rapport bespraken gaat ook in op de opslag en verwerking van persoonsgegevens. Het bepaalt hierover dat wanneer een overheidsorganisaties zoals in het JenV-domein gebruikmaken van een publieke

cloudoplossing, opslag en verwerking van persoonsgegevens in dit kader moeten voldoen aan privacy-vereisten uit de AVG.

Hieronder valt ook het voldoen aan vereisten inzake doorgiften van persoonsgegevens. In ieder geval moet worden voldaan aan één van de onderstaande vereisten:

a) opslag en verwerking binnen de Europese Economische Ruimte (EER);
b) in landen waarvoor een adequaatheidsbesluit bestaat;
c) op basis van een passend doorgiftemechanisme dat voldoet aan de vereisten (van art. 46, hoofdstuk V) van de AVG, zoals een modelcontract (SCC).

Toelichting
Hoewel enkel een voorbeeld van een commerciële leverancier van spraakherkenningstechnologie en clouddiensten, blijkt uit interviews die Considerati heeft gevoerd met JenV medewerkers dat de overheid afspraken heeft gemaakt met Microsoft over de opslaglocatie van de gegevens. Met Microsoft is afgesproken dat de persoonsgegevens worden opgeslagen op servers binnen de EER zodat van doorgifte van persoonsgegevens in principe geen sprake is. Hiermee wordt aan het hierboven genoemde vereiste a) voldaan.

CLOUD Act

Indien de persoonsgegevens die JenV met een commerciële leverancier deelt worden opgeslagen binnen de EER is er in beginsel geen sprake van doorgifte. Wel speelt hier mogelijk nog andere wetgeving een rol: de Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Deze wet regelt elektronisch bewijs in strafzaken en bepaalt dat Amerikaanse autoriteiten bij Amerikaanse clouddienstverleners gegevens mogen opvragen die in een ander land zijn opgeslagen. Het gaat hierbij om allerlei soorten gegevens waaronder audio-opnames en transcripten. Het betreft hier dus niet een wet waar JenV onder valt, maar wetgeving waar Amerikaanse aanbieders onder vallen. Voor gevoelige verwerkingen waarbij gebruikt wordt gemaakt van Amerikaanse commerciële aanbieders is het van belang om te beschouwen wat de potentiële impact van deze wetgeving is.

7 Analyse (juridische) risico's spraakherkenning binnen Justitie en Veiligheid

7.1 Risico's spraakherkenning binnen het domein Justitie en Veiligheid

De inzet van spraakherkenningstechnologie brengt mogelijk (privacy)risico's met zich mee. In dit hoofdstuk schetsen we mogelijke risico's van de inzet van spraakherkenning. Hierbij kijken we breder dan het recht op privacy en gegevensbescherming. Wanneer het gaat om hoog-risico verwerkingen, adviseren wij om een DPIA en indien nodig een andere risicoanalyse zoals een mensenrechtentoets uit te voeren.

7.1.1 Incomplete of incorrecte transcripties

Net als geschreven verslagen is een transcript op basis van spraakherkenning niet feilloos. Een transcriptie op basis van spraakherkenning kan incompleet of incorrect zijn. Fouten in transcriptie kunnen vele oorzaken hebben: het model kan woorden niet herkennen, er is te veel achtergrondgeluid et cetera. Ook is het mogelijk dat spraak niet wordt toegewezen aan de juiste persoon.[71]

Wanneer er geen maatregelen zijn getroffen om fouten te herkennen (zoals handmatige controle achteraf) dan kunnen op basis van incorrecte of incomplete transcripties verkeerde conclusies worden getrokken. De ernst van verkeerde beslissingen genomen op basis van een incorrecte of incomplete auto-transcriptie zijn afhankelijk van de concrete contexten waarbinnen auto-transcriptie wordt toegepast.

7.1.2 Uitsluiting van bepaalde groepen

Afhankelijk van hoe het spraakherkenningsmodel is getraind, kan spraakherkenning meer of minder effectief zijn voor bepaalde talen en dialecten. Denk bijvoorbeeld aan personen die de Nederlandse taal minder goed machtig zijn en tijdens een verhoor woorden uit hun eigen taal of onbekende straattaal gebruiken die niet worden herkend door het spraakherkenningssysteem.

[71] De kans hierop is afhankelijk van de genomen maatregelen. Wanneer bijvoorbeeld aparte audiokanalen worden gebruikt voor iedere persoon dan is de kans hierop laag.

Een hogere foutgevoeligheid of het überhaupt niet werken van het spraakherkenningsmodel kan tot de uitsluiting van bepaalde groepen bij de inzet van spraakherkenning. Dit risico is niet uniek aan de inzet van spraakherkenning en kan zich ook voordoen waar menselijke notulisten transcriberen. Omdat spraakherkenningsmodellen niet onfeilbaar zijn, is het van belang om dit risico te identificeren en maatregelen te implementeren om het risico zo veel mogelijk te beperken. De aard en de ernst van dit risico is afhankelijk van de organisatorische inbedding. Welke maatregelen zijn er bijvoorbeeld om fouten te herkennen en te herstellen en welke alternatieven zijn er naast spraakherkenning in het proces.

7.1.3 Ontbreken nuance en context

Bij auto-transcriptie wordt het gesproken woord letterlijk vertaald naar een geschreven tekst. Hierdoor kan zonder aanvullende menselijke interventie een hoop van de context van een gesprek verloren gaan. Daar waar een mens (bijvoorbeeld een verbalisant) belangrijke context kan weergeven in een verslag, is dit bij een computer niet het geval.[72] Een spreker kan bijvoorbeeld angstig of boos zijn, of een opmerking grappig of cynisch bedoelen. Deze context kan bijzonder relevant zijn voor de interpretatie van wat er gezegd is. Het onvoldoende meenemen van de context van het gesprek kan tot een verkeerd beeld leiden van een persoon of zelfs tot een verkeerde interpretatie van iemands woorden.

7.1.4 Mission creep en function creep

Bij de toepassing van spraakherkenning of autotranscriptie wordt spraak omgezet in tekst. Zoals we in hoofdstuk 2 van dit rapport bespraken, bestaan er meerdere subcategorieën van spraaktechnologie. In die zin kan spraak bijvoorbeeld niet enkel gebruikt worden om een transcriptie te produceren (spraakherkenning en autotranscriptie), maar ook om sprekers te identificeren (sprekerherkenning). Met name aan deze laatste technologie kleven hoge risico's voor betrokkenen en gelden strengere juridische vereisten. Zo geldt vanuit een privacyrechtelijk oogpunt dat spraak als een biometrisch gegeven kwalificeert.[73] Zolang spraak echter niet wordt gebruikt om een individu te identificeren, bijvoorbeeld in het geval van spraakherkenning en autotranscriptie, kwalificeert dit biometrisch gegeven

[72] Er zijn wel AI-toepassingen die emoties kunnen herkennen op basis van stem en/of gezichtsuitdrukking.
[73] Zie paragraaf 4.2.3. voor een nadere uitleg van de classificatie van spraak als biometrisch gegeven vanuit privacyrechtelijk perspectief.

niet als een bijzondere categorie persoonsgegevens in de zin van de AVG en is hierop het strengere regime van artikel 9 AVG dus niet van toepasing. Waar spraak echter wordt gebruikt voor het identificeren van personen, kwalificeert het wel als een bijzonder persoonsgegevens in de zin van de AVG. In dat geval zal de verwerking hiervan in beginsel verboden zijn tenzij aan een van de voorwaarden in artikel 9 lid 2 AVG voldaan wordt. Tot slot bepaalt ook de Wpg (artikel 5) dat ten aanzien van de verwerking van bijzondere categorieën persoonsgegevens strengere voorwaarden gelden (zie paragraaf 4.2.3.).

Naast het privacyrechtelijk perspectief, omvat ook de concept AI Verordening bijzondere regelingen voor AI-systemen die op identificatie gericht zijn. Zo geldt in eerste instantie dat dergelijke systemen als hoog-risico systemen kwalificeren, maar daarnaast schetst deze wet ook bepaalde contexten waarin identificatie middels AI tot de categorie 'verboden praktijken' wordt gerekend (zie paragrafen 5.1.1. en 5.1.2.).

Zo bezien kan spraak voor andere doeleinden worden ingezet dan voor spraakherkenning alleen. Dit kan in de praktijk leiden tot *mission creep*. Dit doet zich voor wanneer informatie wordt gebruikt voor een ander doel dan het oorspronkelijk gespecificeerde doel. Met andere woorden, er bestaat een risico dat spraak voor steeds meer toepassingen wordt verwerkt en voor andere doeleinden dan waarvoor het in eerste instantie is verzameld. Dit kan botsen met het beginsel van doelbinding dat in artikel 5 AVG is neergelegd, tenzij er sprake is van verenigbaarheid met het oorspronkelijk doel van verwerking. Om dit te voorkomen, is het van belang te garanderen dat spraak voor duidelijk omschreven doeleinden wordt verwerkt, dat helder is welke rol spraakherkenning hierbij speelt en dat de verdere verwerking van die spraak voor andere doeleinden verenigbaar is met het oorspronkelijke doel van de verwerking. Waar dit laatste niet het geval is, zal opnieuw de rechtmatigheid van de verwerking getoetst moeten worden.

7.1.5 Beïnvloeding betrokken partijen

De wetenschap dat een gesprek wordt opgenomen en/of volledig getranscribeerd, kan van invloed zijn op het gedrag van personen. Mensen zouden zich bijvoorbeeld minder vrij kunnen uiten in de wetenschap dat alles dat zij zeggen letterlijk wordt weergegeven. Dit

risico is wellicht minder relevant voor toepassingen waar audio sowieso wordt opgenomen (denk bijvoorbeeld aan verhoren), maar voor toepassingen waar normaliter geen opnames en/of transcripties worden gemaakt kan de dynamiek van een gesprek veranderen. Denk bijvoorbeeld aan een vergadering: deelnemers weten dat er een verslag wordt gemaakt, maar een dergelijk verslag is doorgaans geen volledige weergave van het gesprek. Het maken van flauwe grapjes en cynische opmerkingen zou ontmoedigd kunnen worden door auto-transcriptie, maar mogelijk ook het delen van gevoelige informatie of persoonlijke observaties. Ditzelfde zou kunnen gelden voor een getuige: misschien is deze minder bereid om vrijuit te spreken wanneer deze weet dat elk woord wordt vastgelegd (en daarmee dus onderdeel kan worden van het dossier).

7.1.6 Afhankelijkheid spraakherkenning

Wanneer spraakherkenning succesvol blijkt, kan de toepassing ervan een vlucht nemen. Dit is niet alleen een kans maar ook een kwetsbaarheid. Mogelijk zou auto-transcriptie voor bepaalde toepassingen zelfs verplicht kunnen worden. Dit betekent dat de primaire processen in de justitie- en veiligheidsketen in toenemende mate afhankelijk worden van spraakherkenning. Wanneer de spraakherkenning niet goed werkt of tijdelijk niet beschikbaar is, dan kan dit van invloed zijn op het primaire proces.

7.1.7 Gevoelige aard 'normale' persoonsgegevens

Hoewel spraak in principe niet als bijzonder persoonsgegevens kwalificeert, kleven er aan de verwerking hiervan wel risico's voor de betrokkenen. Zo kunnen misbruik en datalekken nog steeds potentieel nadelige gevolgen hebben voor de betrokkenen en daarom dienen extra waarborgen ingebouwd te worden waar spraak wordt verwerkt. Hierbij dient in het bijzonder aandacht te worden besteed aan de inhoud van het gesprek en wat dit over de betrokkene zegt.

7.1.8 Gegevensdeling met partijen buiten de justitie keten

Wanneer gebruik wordt gemaakt van spraakherkenningsmodellen van commerciële partijen, dan is de kans groot dat (gevoelige) gegevens gedeeld moeten worden met deze partijen.[74] Meer specifiek de audio/video opnamen die als trainingsdata en/of inputdata

[74] Het antwoord op deze vraag is afhankelijk van de technische inrichting. Wanneer de infrastructuur van de commerciële partij wordt gebruikt om spraakherkenning mogelijk te maken of spraakherkenningsmodellen in productie te brengen dan

worden gebruikt. Hoewel contractuele afspraken worden gemaakt en deze partijen technische en organisatorische maatregelen implementeren om deze data te beschermen, is niet volledig uit te sluiten dat deze data in te zien zijn door de derde partij. De aard en de ernst van dit risico is afhankelijk van de gevoeligheid van de gegevens en de context waarin de spraakherkenning wordt toegepast.

7.2 Mitigeren risico's spraakherkenning binnen Justitie en Veiligheid

Om de hierboven beschreven risico's weg te nemen of te verkleinen kunnen diverse maatregelen worden getroffen.

7.2.1 Organisatorische maatregelen

Dubbelcheck transcripties

Met het oog op de inrichting van een zorgvuldig proces, is het van belang te voorkomen dat incorrecte of incomplete transcripties tot verkeerde conclusies en beslissingen leiden die rechtsgevolgen hebben voor betrokkenen. Daarom moeten maatregelen getroffen worden om fouten in transcripties te herkennen. Dit kan bijvoorbeeld gerealiseerd worden door een dubbelcheck van transcripties door een handmatige controle achteraf. Door een dergelijke maatregel in te bedden in het beleid rondom de toepassing van spraakherkenning, kan voorkomen worden dat fouten tot onjuiste resultaten leiden.

Aanvullende bescherming gevoelige persoonsgegevens

Omdat spraak, afhankelijk van de context waar het in verwerkt wordt, gevoelige informatie bevat, is het van belang om dit persoonsgegeven hetzelfde niveau van bescherming te bieden als andere persoonsgegevens waar hogere risico's aan kleven, met name bijzondere categorieën persoonsgegevens of strafrechtelijke gegevens. In die zin is het aan te raden spraak bij de ontwikkeling en toepassing van spraakherkenning ten minste als een gevoelig persoonsgegeven te beschouwen en de waarborgen in organisatorische zin hierop in te richten om onnodige risico's te beperken.

Alternatieven waar spraakherkenning tekortschiet

moeten data worden gedeeld met de derde partij. Wanneer een kant- en klaar model wordt genomen en op de eigen infrastructuur wordt gedraaid, dan is dit doorgaans geen risico.

Met het oog op de mogelijke uitsluiting van bepaalde groepen personen bij de toepassing van spraakherkenning, bijvoorbeeld doordat deze de Nederlandse taal niet (voldoende) beheersen, is het van belang te voorkomen dat bepaalde groepen mensen hierdoor onterecht worden buitengesloten en zelfs gediscrimineerd. Dit kan bijvoorbeeld voorkomen wanneer het spraakherkenningsmodel een bepaald dialect onvoldoende herkent. Om dit te voorkomen, is het van belang om alternatieven te bieden waar spraakherkenning tekortschiet. Zo kan bijvoorbeeld voor bepaalde gevallen waarin duidelijk is dat spraakherkenning onvoldoende toereikend is om een correcte en volledige transcriptie te leveren, notulisten/verbalisanten worden ingezet om te notuleren. Ook kan gekeken worden hoe teruggevallen kan worden op de oorspronkelijke audio-opnamen.

Afspraken met derden en een cloudstrategie

Om te voorkomen dat verwerkers buiten de justitieketen onbegrensd toegang hebben tot persoonsgegevens moeten hierover afspraken worden gemaakt in een verwerkersovereenkomst. Daarnaast geldt dat zelfs als een verwerkersovereenkomst is gesloten, bepaalde informatie wegens de gevoeligheid daarvan niet met derden gedeeld kan worden. Zoals we in paragraaf 6.5.2.1. bespraken, bepaalt het Rijksbrede cloudbeleid wanneer en voor welke type gegevens het uitdrukkelijk niet is toegestaan om publieke clouddiensten te gebruiken. Daarbij bepaalt dit beleid verder ook welke voorwaarden op organisatorisch niveau moeten worden geïmplementeerd om een verantwoord gebruik van publieke clouddiensten te garanderen (zie tabel 2). Een van die voorwaarden is om een departementaal cloudbeleid te formuleren. JenV dient een beleid op te stellen en hierin bijvoorbeeld op te nemen welke categorieën persoonsgegevens gedeeld mogen worden met publieke cloudaanbieders in de context van spraakherkenning.

Inbedding in primaire processen

Verder moet het gebruik van spraakherkenning goed worden ingebed in de primaire processen en specifieke risico-beperkende maatregelen worden genomen om de gesignaleerde risico's te beperken. In contexten waar het belang van een zeer accurate transcriptie groot is moeten aanvullende (menselijke) controles worden ingebouwd. Ook

is het van belang om een duidelijke koppeling te behouden tussen de transcriptie en het brondocument zodat in geval van twijfel altijd teruggegrepen kan worden op de originele audio.

Organisatorische maatregelen beveiliging

Om ervoor te zorgen dat toegang tot audio-opnamen wordt beperkt tot diegenen die daartoe gemachtigd zijn dan wel doeleinden die dat rechtvaardigen, is het van belang dat ten aanzien hiervan passende organisatorische maatregelen worden getroffen. Hoewel contractuele afspraken worden gemaakt en betrokken partijen technische en organisatorische maatregelen implementeren om de data afkomstig uit het JenV-domein te beschermen, is niet volledig uit te sluiten dat deze data in te zien zijn door een derde partij die buiten de verhouding verwerkingsverantwoordelijke-verwerker valt. Aangezien het met het oog op de Cloud Act niet kan worden uitgesloten dat Amerikaanse autoriteiten bij het gebruik van Amerikaanse commerciële leveranciers van clouddiensten, zoals Microsoft, toegang kunnen verkrijgen tot gegevens uit het JenV-domein, is het van belang om vanuit een organisatorisch standpunt duidelijkheid te scheppen over welke gegevens onder welke voorwaarden met welke partijen worden gedeeld en welke partijen bij welke gegevens kunnen komen. Beleid hierover kan worden opgenomen in het departementaal cloudbeleid. Overigens geldt dit niet alleen voor Amerikaanse aanbieders, ook voor andere niet Nederlandse aanbieders kan dit relevant zijn.

Transparantie en inzicht in gevolgen

Zoals wij hierboven aangaven, kan de toepassing van spraakherkenning het gedrag van betrokken partijen beïnvloeden. Dit kan zowel invloed hebben op de uiteindelijke uitkomsten voor verdachten alsook voor werknemers binnen het JenV-domein. Om te voorkomen dat vraagstukken rondom spraakherkenning van negatieve invloed zijn op de uitvoer van de primaire processen, is het van belang om bij de toepassing van spraakherkenning transparant te zijn over het gebruik daarvan, de wijze waarop het gebruikt wordt, het doel van het gebruik, de potentiële risico's daarvan en de mitigerende maatregelen die zijn getroffen om risico's te beperken. Op de manier weten betrokkenen

wat zij kunnen verwachten wanneer spraakherkenning wordt toegepast en kunnen mogelijke afstandelijke houdingen ten opzichte van spraakherkenning worden voorkomen.

Representatieve input- en trainingsdata

Om ervoor te zorgen dat een spraakherkenningsmodel naar behoren werkt en in veel verschillende situaties kan worden gebruikt, moet aandacht worden besteed aan de trainingsdata. De trainingsdata moet voldoende representatief zijn en van voldoende kwaliteit. Ook aan de inputdata moet aandacht worden besteed. Bij deze laatste is het met name van belang om over goede kwaliteit audio beschikken en een duidelijk onderscheid tussen sprekers. Bij de eerste *use case* van de politie, spraakherkenning in de context van verhoren, is het van belang dat de verhoorkamers zo worden ingericht dat er een heldere audio opname wordt opgenomen. Bij de andere *use cases* geldt dit uiteraard ook, hoe duidelijker de audio opname, hoe bruikbaarder de input data is voor het spaakherkenningsmodel.

7.2.2 Technische maatregelen

Technische koppeling audio en transcriptie

Om ervoor te zorgen dat de transcriptie makkelijk kan worden gecontroleerd raden we aan om ervoor te zorgen dat in de transcriptie een link wordt gelegd naar de vindplaats in het audiobestand. Bijvoorbeeld: wanneer men twijfelt of een stuk tekst juist is getranscribeerd, wordt deze persoon direct naar de vindplaats in het audiobestand geleid doordat tekst en audio aan elkaar gekoppeld zijn. Deze maatregel maakt het makkelijker om fouten te verbeteren in de transcriptie.

Technische maatregelen beveiliging

Om ervoor te zorgen dat toegang tot audio-opnamen wordt beperkt tot diegenen die daartoe gemachtigd zijn dan wel doeleinden die dat rechtvaardigen, is het van belang dat passende technische maatregelen worden getroffen. Om te voorkomen dat partijen of individuen toegang krijgen tot audiobestanden waartoe zij geen toegang behoren te

verkrijgen dan wel voor andere doeleinden dan waarvoor deze oorspronkelijk bestemd zijn, is het van belang om te kijken in hoeverre bestaande technische maatregelen die zijn getroffen om persoonsgegevens binnen het JenV-domein te beschermen ook volstaan in de context van spraakherkenning. Hierbij moet gedacht worden aan de opslag van gegevens, maar ook aan de veiligheid van de modellen zelf: hoe robuust zijn deze tegen aanvallen en storingen?

Diverse en inclusieve trainingsdata

Om te voorkomen dat door de toepassing van spraakherkenning bepaalde groepen personen worden uitgesloten, is het aan te raden bij het (her)trainen van de modellen voor spraakherkenning te verzekeren dat deze modellen worden getraind aan de hand van trainingsdata die een zo groot mogelijke inhoudelijke diversiteit en inclusiviteit garanderen. In de praktijk betekent dit dat voor de training van het akoestisch model de trainingsdata bijvoorbeeld verschillende toonhoogten en dialecten moeten bevatten. Voor het trainen van het taalmodel betekent dit dat de trainingsdata ook spraak moet bevatten van individuen met een spraak- of stemafwijkingen of spraak van individuen die andere woorden of zinsconstructies gebruiken.

Hoewel het onmogelijk is om te garanderen dat trainingsdata 100% divers en inclusief is, is een zo groot mogelijke mate van diversiteit en inclusiviteit gewenst en draagt dit bij aan de beperking van mogelijke uitsluitingen van bepaalde groepen personen. Waar het niet mogelijk is om diversiteit en inclusiviteit te garanderen, is het van belang dat de menselijke maat wordt gewaarborgd.

Anonimisering / pseudonimisering

Het is van belang om in beginsel geen vertrouwelijke gegevens of gevoelige context te delen die normaliter niet openbaar zijn. Wanneer gegevens gedeeld worden neem in ieder geval de volgende maatregelen:

- Indien mogelijk moeten de gegevens worden geanonimiseerd.

- Waar mogelijk moeten voor de training (beperkte) delen van gesprekken worden gebruikt om te voorkomen dat in de trainingsdata gevoelige inhoud staat betreffende een identificeerbare persoon.
- De gegevens dienen adequaat te worden beveiligd.

8 Conclusie

In opdracht van het Ministerie van JenV, brengen wij in dit rapport aan de hand van verschillende *use cases* binnen het JenV-domein de juridische kaders en voorwaarden in kaart waaronder spraakherkenning verantwoord kan worden toegepast binnen het werkveld van JenV.

Spraakherkenning omvat de automatische omzetting van spraak naar tekst. Als zodanig worden bij de omzetting van spraak persoonsgegevens verwerkt en wordt er gebruikgemaakt van AI-technologie. Op de ontwikkeling en het gebruik van spraakherkenning zijn verschillende juridische kaders van toepassing. Deze kaders stellen onder andere regels ten aanzien van de rechtmatigheid van verwerkingsactiviteiten, bewaartermijnen, voorschriften voor training en samenwerking met derden.

Dit hoofdstuk bevat de conclusies van dit onderzoek en geeft antwoord op de hoofdvraag van dit onderzoek:

"Onder welke juridische voorwaarden kunnen spraakherkenning en autotranscriptie verantwoord worden toegepast binnen het werkveld van Justitie en Veiligheid?"

Deze hoofdvraag valt uiteen in diverse deelvragen. In de volgende paragraaf beantwoorden wij de deelvragen (die elk op hun beurt weer uiteenvallen in subvragen).

8.1 Toestemming

Welke vereisten stellen de juridische kaders aan het vragen van toestemming voor het gebruik van spraakherkenning en autotranscriptie binnen het werkveld van justitie en veiligheid?			
Deelvraag	**Antwoord**	**Wettelijke onderbouwing**	**Vindplaats rapport**
Is er toestemming vereist van deelnemers aan een gesprek wanneer dit (1) wordt opgenomen, (2) door software op basis van de	Toestemming is niet vereist om gebruik te maken van spraakherkenning. Sterker nog, in de meeste gevallen zal toestemming binnen het JenV-domein niet mogelijk zijn omdat toestemming niet voldoet aan de	**AVG** Artikel 6 lid 1 (e) AVG; Artikel 6(f) AVG.	§6.2.

opname wordt getranscribeerd (waarbij de sprekers worden genummerd), en (3) in de transcriptie bij elke passage wordt gemeld wie de spreker is, en (4) de identificatie of authenticatie van de spreker door het systeem wordt uitgevoerd aan de hand van de stem en spraak van personen?	vereisten die de AVG hieraan stelt (vrijelijk gegeven, specifiek, geïnformeerd en ondubbelzinnig). Met name het vereiste dat toestemming vrijelijk moet worden gegeven zorgt ervoor dat toestemming waarschijnlijk niet geldig is. In gevallen waarin een ongelijke verhouding bestaat tussen de betrokkene en de verwerkingsverantwoordelijke, wordt toestemming niet als vrij aangemerkt. De verhouding tussen JenV en de betrokkene (dader, slachtoffer, werknemer) kan als ongelijk worden bestempeld waardoor toestemming niet aan alle vereisten uit de AVG voldoet. In plaats van toestemming kan de verwerking van persoonsgegevens eventueel worden gerechtvaardigd door andere grondslagen uit de AVG, de Wpg en de Wjsg. Per specifieke casus of proces waarvoor spraakherkenning wordt ingezet moet daarom worden beoordeeld – door middel van een legitimiteitstoets - op welke grondslag uit de AVG, Wpg of Wjsg deze verwerking gebaseerd wordt. Hiervoor is nodig dat alle processen verder worden uitgedacht zodat helder is welke persoonsgegevens voor welke specifieke doeleinden en binnen welk juridisch kader worden verwerkt. Voor de politie geldt bijvoorbeeld dat zij zich – afhankelijk van de situatie – kan beroepen op het gerechtvaardigd belang (artikel 6 lid 1(f) AVG) bij interne bedrijfsvoering of op één van de	**Wpg** Artikel 3 Politiewet jo artikelen 8 – 10 Wpg **Wjsg** Artikel 2 Wjsg; Artikel 39 a-b Wjsg; Artikel 40 Wjsg; Artikel 51a Wjsg; Artikel 51e Wjsg.	

	grondslagen uit de Wpg bij de uitvoering van de politietaak. Wanneer de politie de Wpg als grondslag neemt moet zij kunnen onderbouwen dat transcriptie noodzakelijk is om tot een goede uitvoering van de politietaak te komen. Wanneer de politie stelt dat het gebruik van spraakherkenning facilitair van aard is en het werk van de politie eenvoudiger en efficiënter maakt zou spraakherkenning toegepast kunnen worden in het kader van de interne bedrijfsvoering waarop niet de Wpg maar de AVG van toepassing is. Per casus of proces waarvoor JenV spraakherkenning inzet, dient te worden beoordeeld of de verwerking gebaseerd moet worden op artikel 6 lid 1sub f AVG of op één van de grondslagen uit de Wpg.		
In hoeverre is daarin verschil tussen de inzet van een menselijke notulist of een geautomatiseerd systeem?	Er zijn verschillen tussen menselijke en machinale transcriptie die van invloed zijn op de legitimiteit van de inzet van spraakherkenning (lees: risico's, zie hoofdstuk 7.1). Alhoewel het voor het bepalen van de grondslag geen verschil maakt of dit door een mens of door een machine gebeurt, kunnen deze risico's wel een rol spelen bij de noodzakelijkheidstoets: het beoordelen van de proportionaliteit en subsidiariteit, die de uiteindelijke legitimiteit van de betreffende verwerking(en) bepaalt.	idem	§7.1.
Dient toestemming uitdrukkelijk schriftelijk of expliciet ondubbelzinnig gegeven te worden? Of	Zoals uit het bovenstaande volgt, is toestemming in principe geen geschikte grondslag voor de inzet van spraakherkenning binnen het JenV-	**AVG** Artikel 6 lid 1 (a) AVG; Artikel 7 AVG.	§4.2.2. §6.2.1.

volstaat het de deelnemers hier actief of passief op attent te maken?	domein. In de (beperkte) gevallen waarin toestemming als grondslag dient moet deze specifiek en geïnformeerd zijn. De betrokkene moet door middel van een ondubbelzinnige wilsuiting kenbaar maken de toestemming te geven. Uitdrukkelijke toestemming is alleen noodzakelijk wanneer er sprake is van de verwerking van bijzondere persoonsgegevens. Voor een geldige toestemming moet de betrokkene: 1) weten dat om toestemming wordt gevraagd, 2) begrijpen waar hij of zij toestemming voor geeft en 3) weten op welke manier de toestemming moet worden gegeven. De wijze waarop toestemming wordt gegeven moet vervolgens ondubbelzinnig zijn: er moet geen twijfel zijn dat de handeling van de betrokkene een toestemming inhoudt. Daaraan zijn verder geen expliciete vormvereisten verbonden (zoals schriftelijkheid).		
Wat als een van de gespreksdeelnemers (in een gesprekssituatie met meerdere personen) niet opgenomen wil worden? Kunnen spraakherkenning en autotranscriptie dan überhaupt niet ingezet worden? Kan dit bijv. ondervangen worden door de naam van een spreker niet te vermelden bij de gesprekspassages die van de spreker afkomstig zijn?	Wanneer de JenV organisatie zich op toestemming beroept kan zonder die toestemming niet van spraakherkenning gebruik worden gebruikt. Wanneer de JenV-organisatie die gebruikmaakt van spraakherkenning zich op een grondslag uit het op die organisatie toepasselijk regime (AVG, Wpg, Wjsg) kan beroepen is het niet nodig om in aanvulling hierop toestemming van de betrokkene te verkrijgen. In beginsel kan de spraak dus worden opgenomen en getranscribeerd zonder toestemming.	**AVG** Artikel 6 lid 1 (a) AVG; Artikel 6 AVG; Artikel 6 lid 1 (e) AVG. Artikel 21 AVG **WPG** Artikel 8 Wpg.	§4.2.2. §6.2.1.

	Houd er daarbij wel rekening mee dat de betrokkene op grond van de AVG een recht op bezwaar heeft (een opt-out) dat mogelijk gehonoreerd moet worden.		

8.2 Gegevensopslag

Welke vereisten c.q. beperkingen stellen de juridische kaders aan het opslaan van integrale audio-opnames van gesprekken en letterlijke (door tussenkomst van een menselijke notulist of met behulp van spraakherkenningssoftware gegenereerde) transcripties daarvan?			
Deelvraag	**Antwoord**	**Wettelijke onderbouwing**	**Vindplaats rapport**
Onder welke voorwaarden mogen audio-opnames van gesprekken integraal bewaard worden? Welke bewaartermijn is daaraan verbonden?	De audio opnamen mogen worden bewaard zo lang als dat noodzakelijk is voor de doeleinden van de verwerking. Wat de bewaartermijnen zijn is afhankelijk van het wettelijk kader (zie hiernaast) en de concrete toepassing. **AVG:** De AVG bepaalt niet wat de specifieke bewaartermijn voor persoonsgegevens is. Het uitgangspunt is dat persoonsgegevens niet langer mogen worden verwerkt dan noodzakelijk is om de doeleinden te bereiken. Organisaties waarop de AVG van toepassing is, zoals de Reclassering bepalen zelf hoe lang het nodig is om persoonsgegevens (zoals de audio-opnames) te bewaren om de voorgenomen doeleinden te bereiken. **Wpg** Wanneer het gaat om het bewaren van politiegegevens is de Wpg van toepassing. In artikel 4 lid 2 Wpg staat dat de	**AVG** Artikel 5 lid 1 sub c AVG. **Wpg** Artikel 8 lid 6 Wpg; Artikel 9 lid 4 Wpg; Artikel 10 lid 6 Wpg; Artikel 12 lid 6 Wpg; Artikel 14 Wpg. **Wjsg** Artikel 3 lid 7 Wjsg; Artikel 4 Wjsg; Artikel 6 Wjsg; Artikel 41 Wjsg; Artikel 19	§6.3.1. §6.3.2. §6.3.3. §6.3.4.

	verwerkingsverantwoordelijke de nodige maatregelen treft om te verzekeren dat politiegegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verwerkt of dit door enige wettelijke bepaling wordt vereist. De Wpg maakt een onderscheid tussen het verwijderen en vernietigen van gegevens. De Wpg spreekt van het verwijderen van politiegegevens waar politiegegevens slechts minder toegankelijk worden gemaakt, terwijl zij van vernietiging van politiegegevens spreekt waar deze permanent en volledig ontoegankelijk zijn. De Wpg bevat bewaartermijnen die gekoppeld zijn aan de doelen waarvoor de politiegegevens worden gebruikt. **Wjsg** De Wjsg schrijft vaste bewaartermijnen voor persoonsgegevens voor. Artikel 3 lid 7 Wjsg stelt dat de Minister van Veiligheid en Justitie de nodige maatregelen treft om te verzekeren dat justitiële gegevens worden verwijderd of vernietigd zodra deze niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verwerkt of waar dit door enige wettelijke bepaling wordt vereist. Zo is het mogelijk dat voor bepaalde categorieën Wjsg-gegevens specifieke bewaartermijnen gelden die in de Wjsg worden gespecificeerd. Of er een specifiek bewaartermijn geldt hangt dus af van de categorie Wjsg-gegeven die wordt verwerkt.	Wjsg; Artikel 51g Wjsg. **Archiefwet** Selectielijst van het Ministerie van Justitie en Veiligheid en rechtsvoorgangers vanaf 5 mei 1945.	

Hoe ligt dat voor een (automatisch gegenereerd) transcript, verslag of samenvatting op basis van die audio-opname?	Hiervoor gelden dezelfde voorwaarden als hierboven beschreven. Met het oog op het feit dat auto-transcriptie niet onfeilbaar is, is het verstandig om zowel de audio-opname als de transcriptie van het gesprek te bewaren zolang dat nodig is voor de doelen van de verwerking.	**AVG** Artikel 5 lid 1 sub c AVG. **Wpg** Artikel 8 lid 6 Wpg; Artikel 9 lid 4 Wpg; Artikel 10 lid 6 Wpg; Artikel 12 lid 6 Wpg; Artikel 14 Wpg. **Wjsg** Artikel 3 lid 7 Wjsg; Artikel 4 Wjsg; Artikel 6 Wjsg; Artikel 41 Wjsg; Artikel 19 Wjsg; Artikel 51g Wjsg. **Archiefwet** Selectielijst van het Ministerie van Justitie en Veiligheid en rechtsvoorgangers vanaf 5 mei 1945.	§6.3.1. §6.3.2. §6.3.3. §6.3.4.
Hoe ligt dat voor metadata van een gesprek,	Metadata omvatten gegevens die de context, de inhoud en de structuur van	**AVG**	§6.3.1. §6.3.2.

bijvoorbeeld (maar niet beperkt tot) de plaats en tijd van het gesprek of gesprekspassages en/of namen van gespreksdeelnemers?	informatieobjecten – hier: audio-opnames – beschrijven. Zo omvatten metadata onder meer informatie over locaties, duur, tijdstip en bestandsformaat van audio-opnames. Als zodanig geven metadata context aan audio-opnames die door middel van spraakherkenning worden omgezet in transcripten. Hoewel metadata niet op individueel niveau als persoonsgegeven kwalificeren, kunnen deze gegevens in combinatie met andere persoonsgegevens gebruikt worden om een individu te identificeren en herleiden. Als algemene regel gelden daarom dat voor metadata dezelfde vereisten en voorwaarden voor bescherming zoals hierboven beschreven. Ook hier moet dus worden vastgesteld of de opslag van de metadata noodzakelijk is voor het doel van de verwerking. Wanneer dit het geval is mogen deze gegevens in beginsel net zo lang worden bewaard als de audio opnamen en/of het transcript.	Artikel 5 lid 1 sub c AVG. **Wpg** Artikel 8 lid 6 Wpg; Artikel 9 lid 4 Wpg; Artikel 10 lid 6 Wpg; Artikel 12 lid 6 Wpg; Artikel 14 Wpg. **Wjsg** Artikel 3 lid 7 Wjsg; Artikel 4 Wjsg; Artikel 6 Wjsg; Artikel 41 Wjsg; Artikel 19 Wjsg; Artikel 51g Wjsg. **Archiefwet** Selectielijst van het Ministerie van Justitie en Veiligheid en rechtsvoorgangers vanaf 5 mei 1945.	§6.3.3. §6.3.4.

8.3 Training van systemen

Welke vereisten c.q. beperkingen stellen de juridische kaders aan het trainen van spraakherkenning met dergelijke trainingsdata?

Deelvraag	Antwoord	Wettelijke onderbouwing	Vindplaats rapport
Onder welke voorwaarden mogen audio-opnames van gesprekken integraal bewaard worden? Welke bewaartermijn is daaraan verbonden?	Audio opnamen die worden gebruikt voor het (her)trainen van een spraakmodel mogen worden bewaard zo lang als noodzakelijk is voor de doeleinden van de training. Dit betekent dat wanneer de gegevens niet meer noodzakelijk zijn voor de beschreven doeleinden, zij dienen te worden verwijderd. Wanneer het noodzakelijk is om de trainingsdata langer te bewaren (bijvoorbeeld voor het trainen van toekomstige modellen) dan moet onderbouwd worden waarom dit belang zwaarder weegt dan de privacy van de betrokkenen. Wanneer opnamen worden gebruikt die zijn gemaakt in het kader van de uitvoering van de taken van de organisatie in het justitie- en veiligheidsdomein (bijvoorbeeld in het kader van een verhoor) dan moeten deze dat zo lang worden bewaard als in de relevante wetten voorgeschreven. Dit kan soms wel 15 jaar zijn. Wanneer men deze data wil gebruiken voor het trainen van spraakherkenningsmodellen moet onderbouwd worden waarom deze	**AVG** Artikel 5 lid 1 sub c AVG. **Wpg** Artikel 8 lid 6 Wpg; Artikel 9 lid 4 Wpg; Artikel 10 lid 6 Wpg; Artikel 12 lid 6 Wpg; Artikel 14 Wpg. **Wjsg** Artikel 3 lid 7 Wjsg; Artikel 4 Wjsg; Artikel 6 Wjsg; Artikel 41 Wjsg; Artikel 19 Wjsg; Artikel 51g Wjsg. **Archiefwet** Selectielijst van het Ministerie van Justitie en Veiligheid en rechtsvoorgangers vanaf 5 mei 1945.	§6.3.1. §6.3.2. §6.3.3. §6.3.4.

	verwerking (het trainen) verenigbaar is met de oorspronkelijke verwerking.		
Onder welke voorwaarden is het toegestaan om bovengenoemde integrale audio opnamen, of (zins)passages daaruit, en de letterlijke transcriptie daarvan te gebruiken om een spraakherkenningssysteem te trainen?	Wanneer dit: 1) Past binnen de doelomschrijving van het primaire proces waarin de audio opnamen zijn gemaakt; of 2) De nieuwe verwerking (training) verenigbaar is met de oorspronkelijke verwerking; of 3) Wanneer de verwerking niet verenigbaar is en er sprake is van een wettelijke regeling die dit mogelijk maakt (bijvoorbeeld in de Wpg of de Wjsg) of de betrokkene toestemming heeft gegeven. Dus dit betekent dat er specifiek in een wettelijke bepaling moet staan dat gegevens gebruikt mogen worden voor trainingsdoeleinden.	**AVG** Artikel 5 lid 1 sub b AVG; Artikel 6 lid 4 AVG; Artikel 6 lid 1 AVG; Artikel 89 lid 1 AVG. **Wpg** Artikel 3 Politiewet; Artikel 8 Wpg; Artikel 3 lid 3 Wpg; Artikel 6 lid 1 sub f AVG; Artikel 16-24 Wpg; **Wjsg** Artikel 3 lid 6 Wjsg; Artikel 6 lid 1 sub f AVG.	§6.4.1.1. §6.4.2.1. §6.4.3.1.
Wanneer trainingsdata worden 'geknipt' in audio-opnames en bijbehorende transcriptie van losse letters of lettergrepen, woorden of (kleine) woordcombinaties die niet meer herkenbaar zijn als een zin of te traceren zijn tot de inhoud van een gesprek, zijn deze trainingsdata dan nog aan te merken als	Wanneer de trainingsdata niet langer herleidbaar zijn tot een natuurlijke persoon, of dit een onevenredige inspanning vergt, dan is er niet langer sprake van de verwerking van persoonsgegevens. De vereisten vanuit het gegevensbeschermingsrecht (AVG, Wpg, Wjsg) zijn dan niet langer van toepassing. Wanneer geknipte spraakfragmenten echter wel herleidbaar zijn tot een natuurlijk persoon of het niet een onevenredige	Zie bijvoorbeeld artikel 4 onder 1 AVG.	§4.2.1.

persoonsgegevens en geldt in dit geval afwijkende regelgeving? Zo ja, welke regelgeving? Wat betekent dat voor o.a. toestemmingsvereisten en bewaartermijn?	inspanning vergt om deze geknipte fragmenten aan een persoon te koppelen, is er nog wel sprake van persoonsgegevens. In dat geval zijn alle vereisten vanuit het gegevensbeschermingsrecht van toepassing.		
Geldt er eventueel een 'gerechtvaardigd belang' voor het trainen van systemen voor de inzet van spraakherkenning en/of autotranscriptie vanuit het oogpunt van bedrijfsvoering of statistische analyse?	Ja. Vanuit juridisch perspectief kan op twee manieren tegen de verwerking van persoonsgegevens door middel van spraakherkenning worden gekeken: 1) spraakherkenning wordt gezien als onderdeel van het primaire proces (bijvoorbeeld de opsporing) en gebruikt dezelfde grondslag, of spraakherkenning wordt gezien als een maatregel om de efficiency en kwaliteit van de primaire processen te verbeteren. In dat geval biedt artikel 6 lid 1 sub f AVG een mogelijke grondslag omdat het dan gaat om de interne bedrijfsvoering. Hoewel er argumenten zijn voor beide interpretaties, is Considerati van mening dat het beter is om spraakherkenning te zien als onderdeel van het primaire proces omdat de gegevens dan binnen hetzelfde juridische regime verwerkt worden en er daarmee uniformiteit is in de bescherming van persoonsgegevens.	Artikel 6 lid 1 (f) AVG.	§6.4.1.1
Onder welke voorwaarden kunnen organisaties in het JenV-domein en daarbuiten gebruikmaken van elkaars	Organisaties in het JenV-domein en daarbuiten kunnen gebruik maken van elkaars trainingsdata mits wordt voldaan aan de voorwaarden die de	**AVG** Artikel 6 lid 1 AVG; Artikel 5 lid 1 (b) AVG.	§6.5.1 §6.4.1.2. §6.4.2.2. §6.4.3.2.

trainingsdata ten behoeve van het trainen van taalmodellen die worden ingezet om opnames van spraak (gesprekken, verhoren, gesproken taal) door een geautomatiseerd systeem om te zetten in geschreven tekst.	toepasselijke wetgeving hieraan stelt. Dit hangt dus af van welk juridisch kader op de verwerking van toepassing is. In het bijzonder moet worden gekeken of de gegevens mogen worden verstrekt met het oog op het (nieuwe) doel van training. **AVG** Indien de AVG van toepassing is geldt dat organisaties in het JenV-domein en daarbuiten gebruik mogen maken van elkaars trainingsdata indien partijen een grondslag (artikel 6 AVG) hebben op basis waarvan de gegevens worden verwerkt. Daarnaast is het van belang dat een verenigbaarheidstoets wordt uitgevoerd op het doel van de verwerking. De gegevens die worden gebuikt voor het trainen van een spraakherkenningssysteem worden namelijk in eerste instantie doorgaans voor een ander doel verzameld. Een verdere verwerking is alleen toegestaan indien de doeleinden verenigbaar zijn. Of het delen van de gegevens verenigbaar is hangt af van de concrete context en de toegepaste waarborgen. Gevoelige contexten die normaliter niet openbaar zijn of zelfs vertrouwelijk lenen zich doorgaans niet voor het delen van gegevens met derden. De volgende waarborgen / randvoorwaarden zijn in ieder geval van belang:	**WPG** Artikel 15-24 Wpg **Wjsg** Artikel 3 lid 6 Wjsg.	

	• Gegevens moeten worden geanonimiseerd waar mogelijk. • Waar mogelijk moeten voor de training (beperkte) delen van gesprekken worden gebruikt om te voorkomen dat in de trainingsdata gevoelige inhoud staat betreffende een identificeerbare persoon. • De gegevens dienen adequaat te worden beveiligd (onder andere door middel van encryptie, toegangscontrole en/of pseudonimisering. **Wpg** Of het delen van politiegegevens binnen het JenV-domein om een spraakherkenning systeem te trainen is toegestaan hangt ervan af of dit wordt gezien als onderdeel van de politietaak. Indien dit zo is, betekent dit dat de Wpg van toepassing is. De Wpg kent in tegenstelling tot de AVG geen verenigbaarheidstoets. Dit betekent daarom dat wanneer een verwerking van politiegegevens niet binnen de politietaken past, deze verwerking niet is toegestaan. Wat dan nog een optie is, is dat de gegevens door middel van een verstrekking worden 'overgeheveld' naar het AVG regime. Een verstrekkingsgrondslag die mogelijkerwijs in aanmerking kan komen is de verstrekking voor		

	wetenschappelijke en statistische doeleinden (artikel 22 Wpg). De Wpg en het Besluit politiegegevens bieden geen eenduidig antwoord op de vraag of het trainen van spraakherkenningsmodellen mogelijk is op grond van artikel 8 Wpg, of dat het intern overhevelen tussen regimes voor dit doel is toegestaan. Naar onze smaak zou het trainen van spraakherkenningsmodellen binnen de politietaak moeten kunnen vallen. Het eerste argument hiervoor is dat de verwerking ten dienste staat van de uitvoering van de politietaak en de kwaliteit van de gegevensverwerking. Het tweede argument is dat de privacyinbreuk beperkt is, omdat de gegevens enkel worden gebruikt om een model te trainen. Als zodanig is er geen grote impact op de persoonlijke levenssfeer en/of de rechten en vrijheden betrokkenen. Wanneer de gegevens buiten de politie worden gebracht wordt dit argument natuurlijk minder sterk. **Wjsg** De Wjsg, het Besluit justitiële en strafvorderlijke gegevens, de Aanwijzing Wet justitiële en strafvorderlijke gegevens en de AVG bieden geen eenduidig antwoord op de vraag of het trainen van spraakherkenningsmodellen mogelijk is op grond van de Wjsg, of dat het intern		

	overhevelen tussen regimes met het oog op het (her)trainen van modellen voor spraakherkenning binnen het Wjsg-domein is toegestaan. De Wjsg gaat in beginsel over de verwerking van persoonsgegevens (Wjsg-gegevens) die direct verband houden met strafrechtelijke procedures. Doorgaans is dit natuurlijk ook zo, maar bij het (her)trainen van spraakherkenningsmodellen worden deze gegevens op een meer indirecte wijze aangewend voor dit doel, namelijk om in de toekomst de werkzaamheden van justitie eenvoudiger, efficiënter en effectiever te maken. De vraag is in hoeverre de Wjsg deze ruimte biedt. Indien de route van de verenigbaarheidstoets wordt bewandeld, dan moet per proces en per type Wjsg-gegeven worden aangetoond dat de verdere verwerking van Wjsg-gegevens met het oog op het (her)trainen van de modellen voor spraakherkenning aan deze verenigbaarheidstoets voldoet, hoewel er onduidelijkheid bestaat over de mate waarin deze toets ook van toepassing is op Wjsg-gegevens anders dan justitiële gegevens. Een alternatief houdt in dat de verwerking van persoonsgegevens door de fictieve instantie binnen het justitiedomein met het oog op het (her)trainen van modellen voor		

	spraakherkenning niet valt binnen de reikwijdte van de Wjsg, maar onder de AVG. In dat geval moet de betreffende fictieve instantie binnen het justitiedomein in dat geval de gegevens uit het Wjsg-regime overhevelen naar het AVG regime. Artikel 6f AVG (gerechtvaardigd belang) biedt dan een mogelijke grondslag. Overigens moet ook hierbij wel worden aangetekend dat dit overhevelen tussen het regime van de Wjsg en de AVG geen duidelijke regeling lijkt te kennen. Hoewel Wjsg aldus bepaalt onder welke voorwaarden (bepaalde) Wjsg-gegevens kunnen worden verstrekt, lijkt een interne verstrekking ten behoeve van taken die niet direct aan strafrechtspleging zijn verbonden en ten aanzien van Wjsg-gegevens in zijn algemeenheid, niet expliciet te worden geregeld.		
Binnen de Nederlandse AI Coalitie ontstaat een samenwerkingsverband van bedrijven, overheden, semipublieke instellingen en kennisinstellingen die beogen samen te werken om spraakherkenning voor de Nederlandse taal verder te brengen. Een belangrijk onderdeel hiervan is het 'bijeenbrengen' van trainingsdata van verschillende bovengenoemde partijen. In hoeverre kunnen JenV	De partijen die gegevens ter beschikking stellen voor training van spraakherkenningsmodellen moeten hiervoor een deugdelijke grondslag hebben, zoals bijvoorbeeld toestemming van betrokkenen. Wat de toepasselijke grondslag is moet per proces / dataset worden beoordeeld. Wanneer de verstrekkers van de trainingsdata een grondslag hebben voor de verwerking dan kunnen JenV organisaties deze grondslag hanteren. Omgekeerd geldt hetzelfde: wanneer JenV organisaties een grondslag	**AVG** Artikel 6 lid 1 AVG; Artikel 5 lid 1 (b) AVG. **WPG** Artikel 15-24. **Wjsg** Artikel 3 lid 6 Wjsg.	§6.5.1 §6.4.1.2. §6.4.2.2. §6.4.3.2.

organisaties voor het trainen van hun software gebruik maken van trainingsdata van zulke derde partijen? In hoeverre mogen derde partijen gebruik maken van trainingsdata van JenV organisaties voor het trainen van hun software? Hoe ligt dit wanneer het gaat om leveranciers van spraakherkenningssoftware? Gelden hier in juridische zin op grond van wet en regelgeving nog andere beperkingen?	hebben voor het delen, dan mogen de organisaties deze gegevens voor het trainen van modellen gebruiken. Dit is voor leveranciers niet anders. Wel dient er bij die laatste categorie in het bijzonder rekening mee te worden gehouden dat de gegevens niet worden gedeeld met landen zonder een adequaat beschermingsniveau voor gegevensbescherming (gegevensexport). Houd er hierbij wel rekening mee dat de JenV context doorgaans zeer gevoelig is en er geen toestemming kan worden gevraagd aan de betrokkenen. Het is ook onwaarschijnlijk dat het verstrekken aan een grote groep publieke en private partijen verenigbaar is met de oorspronkelijke verwerkingsdoelen (zelfs wanneer onderbouwd kan worden dat dit voor wetenschappelijke doeleinden is). Zolang de gegevens niet geanonimiseerd kunnen worden moet zéér terughoudend worden omgesprongen met het delen van trainingsdata met derde partijen, zeker buiten de justitieketen. Het ontwikkelen van een gezamenlijk taalmodel voor de Nederlandse taal kan van groot belang zijn voor Nederland. Betoogd kan worden dat het hiermee gaat om een ‘zwaarwegend algemeen belang’. In de nieuwe AI Verordening is een voorstel		

	gedaan om het doelbindingscriterium los te mogen laten voor verwerkingen met een zwaarwegend algemeen belang die deelnemen aan een 'regulatory sandbox'. Dit biedt mogelijk richting de toekomst aanvullende mogelijkheden.		

8.4 Afname uit de markt en samenwerking met bedrijven

Zijn er, los van kwalitatieve of economische overwegingen, in juridische zin beperkingen aan het gebruik van commerciële producten door JenV organisaties?

Deelvraag	**Antwoord**	**Wettelijke onderbouwing**	**Vindplaats rapport**
Binnen Nederland wordt op het gebied van spraakherkenning en autotranscriptie ook samengewerkt tussen bedrijven, overheden, semipublieke instellingen en kennisinstellingen om deze technologie voor de Nederlandse taal verder te ontwikkelen. Een belangrijk onderdeel hiervan is het 'bijeenbrengen' van trainingsdata van verschillende bovengenoemde partijen. In hoeverre kunnen JenV-organisaties, voor het trainen van hun software, op een juridisch verantwoorde manier gebruik maken van trainingsdata van zulke derde partijen? In hoeverre mogen	Vanuit het perspectief van gegevensbescherming bestaan er geen specifieke bezwaren tegen het gebruiken van spraakherkenningsmodellen van derden (inclusief commerciële partijen). Voor wat betreft trainingsdata van derde partijen moet JenV een grondslag hebben voor het verwerken van deze data. Bij het gebruik van modellen en trainingsdata van derden is het wel van groot belang hoe de technische en organisatorische inrichting is. Wanneer het model bijvoorbeeld 'as a service' wordt aangeboden, dan geldt dat deze partij verwerker is (voor de input data). Ditzelfde geldt wanneer een derde partij een platform aanbiedt voor het trainen en in productie brengen van modellen (trainingsdata en input data). Voor het versturen van persoonsgegevens naar deze partijen (trainingsdata en/of	**AVG:** Artikel 28 AVG; Artikel 44 – 50 AVG. **Wpg** Artikel 17a Wpg. **Wjsg** Artikel 16a Wjsg.	§6.5.2

derde partijen gebruik maken van trainingsdata van JenV-organisaties voor het trainen van hun software? Hoe ligt dit wanneer het gaat om leveranciers van spraakherkenningssoftware? Gelden hier op grond van wet- en regelgeving nog andere beperkingen?	input data) gelden de regels van de AVG. Meer specifiek met betrekking tot verwerkers, beveiliging en gegevensdoorgifte buiten Europa. Daarnaast moet aangesloten worden bij de Rijksbrede strategie voor het gebruik van clouddiensten en de beveiligingsvereisten zoals vastgelegd in onder andere de BIO. Hierin is onder meer bepaald dat het uitdrukkelijk niet is toegestaan om clouddiensten te gebruiken voor staatsgeheim gerubriceerde informatie.		

8.5 Overig

Zijn er nog overige zaken waar bij de toepassing van spraakherkenning binnen het JenV-domein rekening mee moet worden gehouden?

Deelvraag	**Antwoord**	**Wettelijke onderbouwing**	**Vindplaats rapport**
Welke vereisten c.q. beperkingen stellen de juridische kaders aan het gebruik van gespreksopnames, bijbehorende transcripties, metadata en op bovenstaande wijze geanonimiseerde trainingsdata voor wetenschappelijk onderzoek? Hoe kan aan die vereisten c.q. beperkingen worden voldaan door maatregelen in beleidsmatige of technische zin?	Voor geanonimiseerde data gelden de regels van het gegevensbeschermingsrecht niet. Voor niet geanonimiseerde gegevens gelden de hierboven beschreven regels (grondslagen, doelbinding et cetera). Wetenschappelijk onderzoek wordt op voorhand gezien als verenigbaar gezien met de oorspronkelijke verwerkingsdoelen. Dit betekent dat wanneer persoonsgegevens die voor andere doelen zijn verzameld voor wetenschappelijke doelen worden gebruikt, dit als verenigbaar wordt	**AVG** Artikel 89 lid 1 AVG. **Wpg** Artikel 22 Wpg. **Wjsg** Artikel 15 lid 1 Wjsg.	---

	gezien en dus is toegestaan. Daarbij geldt wel op grond van artikel 89 AVG dat passende waarborgen moeten worden getroffen (pseudonimisering, beveiliging et cetera). Het is aan te bevelen om dezelfde criteria te hanteren die gelden voor het delen van (gevoelige) JenV informatie met onderzoeksinstellingen in andere contexten. Denk bijvoorbeeld aan het delen van verhoorverslagen met wetenschappers in het kader van criminologisch onderzoek.		
Welke risico's kunnen zich voordoen t.a.v. publieke waarden van bescherming van persoonsgegevens, non-discriminatie en rechtsbescherming bij de inzet van spraakherkenning binnen het werkveld van justitie en veiligheid?	Afhankelijk van hoe het spraakherkenningsmodel is getraind, kan spraakherkenning meer of minder effectief zijn voor bepaalde talen en dialecten. Dit kan mogelijk leiden tot de uitsluiting van bepaalde groepen bij de inzet van spraakherkenning. Dit risico is niet uniek aan de inzet van spraakherkenning en kan zich ook voordoen waar menselijke notulisten transcriberen. De aard en de ernst van dit risico is afhankelijk van de organisatorische inbedding. Welke maatregelen zijn er bijvoorbeeld om fouten te herkennen en te herstellen en welke alternatieven zijn er naast spraakherkenning in het proces.	---	§7.1
Hoe kunnen die risico's worden gemitigeerd door	De benodigde maatregelen zijn afhankelijk van de context.	---	§7.2

maatregelen in beleidsmatige of technische zin?	Allereerst moet aandacht worden besteed aan de accuraatheid en robuustheid van het model. Hierbij vormen de regels voor hoog-risico systemen in de aankomende AI Verordening een goed aanknopingspunt. Deze voorschriften hebben betrekking op de volgende onderwerpen: systeem voor risicobeheer, data en databeheer, technische documentatie, registratie, transparantie en informatieverstrekking, menselijk toezicht, nauwkeurigheid, robuustheid en cyberbeveiliging. Daarnaast moet aandacht worden besteed aan de trainingsdata (deze moet representatief en van voldoende kwaliteit zijn) en aan de input data. Bij deze laatste is het voor een goede performance met name van belang dat de overeenkomst tussen trainingsdata en testdata zo groot mogelijk is. In de praktijk betekent dit dat als er een spraakherkenningsmodel wordt ontwikkeld die gebruikt gaat worden op straat, het beter is om dat model te trainen met spraakmateriaal dat op straat is opgenomen in plaats van 'goede kwaliteit audio' die is opgenomen in een geluidsarme ruimte.		

	Verder moet het gebruik van spraakherkenning goed worden ingebed in de primaire processen en specifieke risico-beperkende maatregelen worden genomen om de gesignaleerde risico's te beperken. In contexten waar het belang van een zeer accurate transcriptie groot is moeten aanvullende (menselijke) controles worden ingebouwd. Ook is het van belang om een duidelijke koppeling te behouden tussen de transcriptie en het brondocument zodat in geval van twijfel altijd teruggegrepen kan worden op de originele audio.		
Mogen opnames van gesprekken die zijn gemaakt met als doel deze gesprekken te laten transcriberen (al dan niet door een geautomatiseerd systeem) ook gebruikt worden om personen in deze gesprekken te identificeren aan de hand van hun spraak (sprekerherkenning) voor opsporingsdoeleinden?	Wanneer de politie op grond van de Wpg spraakherkenning gebruikt (bijvoorbeeld in het kader van de uitvoering van de dagelijkse politietaak, artikel 8 Wpg) dan kunnen de audio opname en transcriptie onder de voorwaarden genoemd in deze artikelen in theorie ook voor de opsporing worden gebruikt (bijvoorbeeld artikel 9 Wpg). Voorts kan de politiegegevens vorderen bij andere JenV organisaties met het oog op de opsporing en deze gebruiken om sprekerherkenning mogelijk te maken. Tevens moet hierbij worden aangetekend dat een dergelijk	**AVG** Artikel 5 lid 1 sub b AVG; Artikel 6 lid 4 AVG. **Wpg** Artikel 3 lid 3 Wpg. **Wjsg** Artikel lid 6 Wjsg.	§4.2.3

	gebruik van gegevens zich moeilijk verhoudt tot de vereisten van artikel 8 EVRM, meer specifiek het vereiste van een duidelijke wettelijke regeling die voldoende waarborgen biedt. Wanneer sprekerherkenning zonder dergelijke waarborgen wordt toegepast, is het namelijk de vraag of de betrokkene dit redelijkerwijs mocht verwachten. Het gebruiken van sprekerherkenning zou daarom dan ook idealiter een eigen (bijzondere) opsporingsbevoegdheid moeten zijn. Wij adviseren nader onderzoek te doen op dit gebied. Waar daarnaast rekening mee gehouden moet worden is dat wanneer biometrische gegevens worden verwerkt met het oog op unieke identificatie (zoals bij sprekerherkenning het geval is) er sprake is van een verwerking van bijzondere persoonsgegevens. Hiervoor geldt dat de JenV organisatie die van srpekerherkenning gebruik wil maken naast een grondslag uit de Avg/Wpg/Wjsg zich ook moet kunnen beroepen op een uitzonderingsgrondslag die een verwerking van bijzondere categorieën van persoonsgegevens rechtvaardigt. Let op dat sprekerherkenning verschilt van sprekerdiarisatie.		

	Sprekerdiarisatie koppelt de verschillende stukjes opgenomen spraak (al dan niet omgezet naar tekst) aan de spreker die deze heeft uitgesproken. Het vaststellen van de precieze identiteit van de spreker is daarvan geen onderdeel waardoor het specifieke regime voor bijzondere categorieën van persoonsgegevens in beginsel niet van toepassing is.		

9 Aanbevelingen voor de praktijk

In dit rapport hebben wij aan de hand van verschillende *use cases* binnen het JenV domein onderzoek gedaan naar de juridische kaders en voorwaarden waaronder spraakherkenning verantwoord kan worden toegepast binnen het werkveld van JenV. Om de analyses uit dit rapport wat meer praktische duiding te geven doen wij in dit hoofdstuk een aantal aanbevelingen voor de praktijk die kunnen bijdragen aan een zorgvuldige toepassing van spraakherkenning en autotranscriptie binnen het JenV-domein.

9.1 Training

Algemeen

- Omschrijf duidelijk het doel voor het trainen van het spraakherkenningsmodel.
- Gebruik in beginsel geen gevoelige, strafrechtelijke en bijzondere persoonsgegevens (zoals persoonsgegevens van kwetsbare verdachte) voor het trainen van het spraakherkenningsmodel, tenzij dit noodzakelijk is voor het goed kunnen trainen van het model.
- Indien gevoelige, strafrechtelijke en bijzondere persoonsgegevens noodzakelijk zijn om het spraakherkenningsmodel te trainen, zorg er dan voor dat identificerende kenmerken (namen, adressen, identificatienummers et cetera) zoveel mogelijk verwijderd worden.
- Zorg ervoor dat het spraakherkenningsmodel wordt getraind met verschillende talen en dialecten om ervoor te zorgen dat het in zoveel mogelijk situaties gebruikt.

Grondslag

- Baseer de training van spraakherkenningsmodellen altijd op een deugdelijke grondslag uit de AVG, Wpg of Wjsg. Houd er rekening mee dat wanneer maatregelen worden genomen om de opnamen niet meer te herleiden naar personen dit niet per definitie betekent dat er geen persoonsgegevens meer worden verwerkt bij het trainen van het spraakherkenningsmodel. Tenzij betoogd kan worden dat de data anoniem zijn (de gegevens kunnen niet of niet anders dan

met een onevenredige inspanning teruggevoerd worden op een persoon), moet er altijd een grondslag zijn voor de verwerking van persoonsgegevens.

- Wanneer persoonsgegevens worden verwerkt, moet de verwerkingsverantwoordelijke hiervoor een grondslag hebben. Wanneer de AVG van toepassing is op verwerking van persoonsgegevens in het kader van het trainen van spraakherkenningsmodellen, dan moet één van de grondslagen uit artikel 6 AVG worden gekozen. Hierbij liggen de uitvoering van de taak van algemeen belang of openbaar gezag (6e AVG) en het gerechtvaardigd belang van de verwerkingsverantwoordelijke (6f AVG) het meest voor de hand. Pas wanneer de grondslagen 6b tot en met f AVG niet van toepassing zijn moet worden gekeken naar de toestemming (zie onder).

- Voor het hebben van een grondslag onder 6e of 6f AVG is het in het bijzonder van belang dat wordt onderbouwd dat spraakherkenning noodzakelijk is om de taken van de organisatie goed uit te voeren.

Toestemming

- Toestemming als grondslag voor het gebruik van persoonsgegevens voor trainingsdoeleinden is alleen mogelijk wanneer deze 'vrij' gegeven kan worden. Dat betekent dat het weigeren van toestemming geen nadelige gevolgen voor de betrokkene mag hebben. Betrokkenen of hun wettelijk vertegenwoordigers mogen ook niet onder druk worden gezet om toestemming te geven. In gevallen waarin een ongelijke verhouding bestaat tussen de betrokkene en de verwerkingsverantwoordelijke, zal toestemming niet snel vrij gegeven kunnen worden. Gebruik van opnamen uit primaire processen in het JenV-domein (verhoren, opnames van rechtszaken, vergaderingen) op basis van toestemming is bijna nooit mogelijk omdat de betrokkenen niet vrij hun toestemming kunnen geven.

Verenigbaarheid

- Wanneer persoonsgegevens, die voor een ander doel zijn verzamelend, worden gebruikt voor het trainen van spraakherkenningsmodellen, onderbouw dan waarom het trainen van het model verenigbaar is met het oorspronkelijke verwerkingsdoel. Houd daarbij rekening met:
    - het verband tussen het oorspronkelijke doel en het nieuwe doel (trainen);
    - de context waarin de gegevens oorspronkelijk zijn verzameld, met name de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke;
    - de aard van de persoonsgegevens, met name of bijzondere persoonsgegevens of strafrechtelijke gegevens worden gebruikt;
    - de mogelijke gevolgen van de nieuwe verwerking voor de betrokkenen;
    - te nemen passende waarborgen, zoals versleuteling en pseudonimisering.

  Voor nadere duiding zie paragraaf 6.4.1.1.

- Stel vast of de persoonsgegevens bewaard moeten blijven voor toekomstig hertrainen van het spraakherkenningsmodel of training van andere modellen. Bepaal (en documenteer) een noodzakelijke termijn voor het opslaan van de gegevens voor het (her)trainen en onderbouw waarom de opslag voor deze termijn noodzakelijk is.

- Leg overwegingen rondom rechtmatigheid, risico's en risico-beperkende maatregelen vast. Wanneer het gaat om hoog-risico verwerking, doe dan een DPIA en indien nodig een andere risicoanalyse zoals een mensenrechtentoets.

9.2 Toepassing

- Stel vast welke 'taak' spraakherkenning moet uitvoeren en binnen welke context dit plaatsvindt.

- Bepaal aan de hand van deze taak en de context wat de -vanuit een privacy perspectief- minst ingrijpende methode om spraakherkenning in te zetten. Bijvoorbeeld: als sprekerherkenning niet noodzakelijk is, kies dan niet voor een systeem dat sprekers herkent.

- Bepaal de grondslag voor het verwerken van persoonsgegevens (de input data) met behulp van spraakherkenning (audio, video met audio). Houd hierbij in het bijzonder rekening met de noodzaak van de toepassing, proportionaliteit en subsidiariteit.

- Informeer betrokkenen over het feit dat er gebruik gemaakt wordt van auto-transcriptie in het gesprek, tenzij de betrokkenen hier reeds van op de hoogte zijn.

- Evalueer het gebruik van spraakherkenning en de effecten die dit heeft op deelnemers aan een gesprek.

- Richt een feedback proces in voor de verbetering van de spraakherkenning om in de toekomst de kans op foutieve transcripties te verkleinen

- Ga ervan uit dat een systeem nooit feilloos is, richt een handmatig, menselijk correctieproces in documenteer dit, zodat er periodiek kan worden beoordeeld of het systeem niet eenzijdig fouten maakt.

- Leg overwegingen rondom rechtmatigheid, risico's en risico-beperkende maatregelen vast. Wanneer het gaat om een hoog-risico verwerking, doe dan een DPIA.

- Bekijk in hoeverre de transcriptie anders is dan het huidige proces en beoordeel de mogelijke effecten daarvan op de deelnemers aan het gesprek. Bijvoorbeeld: wanneer oorspronkelijk alleen een gespreksverslag / samenvatting werd gemaakt: wat verandert er dan door volledige transcriptie?

- Wanneer spraakherkenning breder wordt toegepast dan binnen één context, zorg dan voor heldere criteria voor wanneer spraakherkenning wel of niet gebruikt wordt. Denk bijvoorbeeld aan een onderscheid op basis van de gevoeligheid van een gesprek en/of de deelnemers aan een gesprek.

9.3 Inrichting

- Bij het opnemen van spraak die automatisch getranscribeerd wordt, is het raadzaam om waar mogelijke separate audiokanalen te gebruiken. Het gebruik van separate audiokanalen bij opnamen voor spraakherkenning, verhogen de kwaliteit van de audio en dit verhoogt de kans op een correcte transcriptie. Technische kwaliteit en privacy lopen hierbij gelijk, aangezien het niet langer noodzakelijk is om individuele sprekers te onderscheiden of herkennen met behulp van spraaktechnologie.

- Zorg voor een duidelijke en blijvende koppeling tussen de originele opname (audio of video) en het transcript (opslag van de originele opname én het transcript).

- In die contexten waar het in bijzonder van belang is dat de transcriptie accuraat is (denk aan verslagen van verhoren in strafzaken of tapverslagen) is het van belang om snelle controles van de audio opnamen te faciliteren. Denk bijvoorbeeld aan een transcript met 'time stamps' zodat snel in de originele opname teruggevonden kan worden of wat gezegd is daadwerkelijk getranscribeerd is.

- Wanneer gebruik wordt gemaakt van spraakherkenningsmodellen een spraakherkenningstoolkits van derden (leveranciers, open source) stel dan vast wat de betrokkenheid is van deze derde partijen. Hierbij is het met name van belang om te kijken of zij trainingsdata, input data en output opslaan en/of toegang hebben tot deze data.

- Wanneer derde partijen (bijvoorbeeld leveranciers) betrokken zijn bij de toepassing moet beoordeeld worden of een verwerkersovereenkomst noodzakelijk is.

- Wanneer gegevens worden opgeslagen buiten de Europese Unie / Europese Economische Ruimte moet beoordeeld worden in hoeverre er sprake is van een adequaat niveau van gegevensbescherming. Neem aan de hand van deze beoordeling maatregelen om de gegevensexport te legitimeren.

- Wanneer gebruik wordt gemaakt van cloudopslag of clouddiensten, dient het Rijksbrede Cloudbeleid gevolgd te worden.

- Zorg dat de digitale omgeving waarin het spraakherkenningsmodel wordt gebruikt ingericht is conform de informatiebeveiligingseisen (BIO). Wanneer de toepassing door derden wordt aangeboden, dan dienen ook daar relevante beveiligingsmaatregelen te worden genomen.

10 Literatuurlijst

Wetgeving

Verordening (EU) 2016/679 (Algemene Verordening Gegevensbescherming).

Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (Voorstel AI Verordening).

Richtlijn 2016/680/EG (Richtlijn politie- en justitiegegevens).

Algemene wet bestuursrecht.

Archiefwet 1995.

Wet open overheid.

Wet politiegegevens.

Wet justitiële en strafvorderlijke gegevens.

Innovatiewet Strafvordering.

Selectielijst van het Ministerie van Justitie en Veiligheid en rechtsvoorgangers vanaf 5 mei 1945. Geraadpleegd op 16 september 2022, van https://www.nationaalarchief.nl/sites/default/files/field-file/Selectielijst%20JenV%20vastgesteld%20Stcrt%202021%2017848.pdf

Rechtspraak

EHRM, 6 juni 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. no. 62332/00.

HvJ EU, gevoegde zaken C-92/09 en C-93/02, *Volker und Markus Schecke GbR v. Land Hessen*, conclusie van advocaat-generaal Sharpston, 17 juni 2010.

HvJ EU 20 oktober 2022, *Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2022:805.

HR 29 mei 2009, ECLI:NL:HR:2009:BH4720.

HR 27 juni 2017, ECLI:NL:HR:2017:1166.

Gerechtshof Den Haag 24 december 2019, ECLI:NL:GHDHA:2019:3539.

Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111.

Literatuur

AP. (2016). Cameratoezicht. Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens. Geraadpleegd op 30 november 2022, van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf.

AP. (2019). Advies over het concept voor een wetsvoorstel Modernisering Archiefwet (Archiefwet 2021). Geraadpleegd op 16 september 2022, van https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_modernisering_archiefwet.pdf.

AP. (2020). Toezicht op AI & Algoritmes. Geraadpleegd op 5 april 2022, van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezicht_op_ai_en_algoritmes.pdf.

EDPB. (2020). Guidelines 3/2019 on processing personal data through video devices. Version 2.0. Geraadpleegd op 16 september 2022, van https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.

EDPB. (2021). Guidelines 02/2021 on virtual voice assistants . Version 2.0. Geraadpleegd op 16 september 2022, van https://edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf.

Geijsen, K. (2019), Kwetsbare verdachten tijdens het politieverhoor. Ars Aequi. https://arsaequi.nl/product/kwetsbare-verdachten-tijdens-het-politieverhoor.

O'Shaughnessy, D. (2008). Automatic speech recognition: History, methods and challenges. *Pattern Recognition*, *41*(10), 2965-2979. https://doi.org/10.1016/j.patcog.2008.05.008.

De Vries, in: T&C Algemene Verordening Gegevensbescherming (AVG) inclusief Uitvoeringswet AVG, art. 31 UAVG, aantekening, p. 341.

Websites

Britannica. *Speech | Language, Voice Production, Anatomy, & Physiology*. Geraadpleegd op 5 april 2022, van https://www.britannica.com/topic/speech-language.

Cambridge Dictionary. *Speech definition*. Geraadpleegd op 5 april 2022, van https://dictionary.cambridge.org/dictionary/english/speech. Vertaald vanuit het Engels: 'the ability to talk, the activity of talking, or a piece of spoken language'.

European Union. Aims and values. Geraadpleegd op 16 september 2022, van https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en.

IBM. *Speech Recognition*. Geraadpleegd op 5 april 2022, van https://www.ibm.com/nl-en/cloud/learn/speech-recognition#toc-key-featur-DdHYi0BA.

Pressbooks. How humans produce speech. Geraadpleegd op 5 april 2022, van https://essentialsoflinguistics.pressbooks.com/chapter/2-2-how-humans-produce-speech/#:~:text=Speech%20is%20produced%20by%20bringing,mouth%20and%20nose%20(articulation).

11 Bijlagen

11.1 Bijlage 1: overzicht hoofd- en deelvragen JenV

Hoofdvraag	***Onder welke juridische voorwaarden kunnen spraakherkenning en autotranscriptie verantwoord worden toegepast binnen het werkveld van Justitie en Veiligheid?"***
Deelvraag	*Welke juridische kaders zijn momenteel van toepassing en in hoeverre is de voorgenomen Europese regelgeving van toepassing op spraakherkenning en autotranscriptie?*
Deelvraag	*Welke vereisten c.q. beperkingen stellen de juridische kaders aan het gebruik van spraakherkenning en autotranscriptie binnen het werkveld van justitie en veiligheid?*

Toestemming *Welke vereisten stellen de juridische kaders aan het vragen van toestemming voor het gebruik van spraakherkenning en autotranscriptie binnen het werkveld van justitie en veiligheid?*	1. Is er toestemming vereist van deelnemers aan een gesprek wanneer dit (1) wordt opgenomen, (2) door software op basis van de opname wordt getranscribeerd (waarbij de sprekers worden genummerd), en (3) in de transcriptie bij elke passage wordt gemeld wie de spreker is, en (4) de identificatie of authenticatie van de spreker door het systeem wordt uitgevoerd aan de hand van de stem en spraak van personen?
	2. In hoeverre is daarin verschil tussen de inzet van een menselijke notulist of een geautomatiseerd systeem?
	3. Dient toestemming uitdrukkelijk schriftelijk of expliciet ondubbelzinnig gegeven te worden? Of volstaat het de deelnemers hier actief of passief op attent te maken?
	4. Wat als een van de gespreksdeelnemers (in een gesprekssituatie met meerdere personen) niet opgenomen wil worden? Kunnen spraakherkenning en autotranscriptie dan überhaupt niet ingezet worden? Kan dit bijv. ondervangen worden door de naam van een spreker niet te vermelden bij de gesprekspassages die van de spreker afkomstig zijn?
Gegevensopslag *Welke vereisten c.q. beperkingen stellen de juridische kaders aan het*	5. Onder welke voorwaarden mogen audio-opnames van gesprekken integraal bewaard worden? Welke bewaartermijn is daaraan verbonden?

opslaan van integrale audio-opnames van gesprekken en letterlijke (door tussenkomst van een menselijke notulist of met behulp van spraakherkenningssoftware gegenereerde) transcripties daarvan?	6. Hoe ligt dat voor een (automatisch gegenereerd) transcript, verslag of samenvatting op basis van die audio-opname?
	7. Hoe ligt dat voor metadata van een gesprek, bijvoorbeeld (maar niet beperkt tot) de plaats en tijd van het gesprek of gesprekspassages en/of namen van gespreksdeelnemers?
Training van systemen *Om een spraakherkenningssysteem te trainen is trainingsdata nodig. Bij zgn. 'supervised learning' bestaat deze trainingsdata uit opgenomen audio (stemgeluid, gesproken taal) en de letterlijke (handmatige of geautomatiseerde) transcriptie daarvan. Welke vereisten c.q. beperkingen stellen de juridische kaders aan het trainen van spraakherkenning met dergelijke trainingsdata?*	8. Onder welke voorwaarden is het toegestaan om bovengenoemde integrale audio opnamen, of (zins)passages daaruit, en de letterlijke transcriptie daarvan te gebruiken om een spraakherkenningssysteem te trainen?
	9. Wanneer trainingsdata worden 'geknipt' in audio-opnames en bijbehorende transcriptie van losse letters of lettergrepen, woorden of (kleine) woordcombinaties die niet meer herkenbaar zijn als een zin of te traceren zijn tot de inhoud van een gesprek, zijn deze trainingsdata dan nog aan te merken als persoonsgegevens en geldt in dit geval afwijkende regelgeving? Zo ja, welke regelgeving? Wat betekent dat voor o.a. toestemmingsvereisten en bewaartermijn?
	10. Geldt er eventueel een 'gerechtvaardigd belang' voor het trainen van systemen voor de inzet van spraakherkenning en/of autotranscriptie vanuit het oogpunt van bedrijfsvoering of statistische analyse?
	11. Onder welke voorwaarden kunnen organisaties in het JenV-domein en daarbuiten gebruik maken van elkaars trainingsdata ten behoeve van het trainen van taalmodellen die worden ingezet om opnames van spraak (gesprekken, verhoren, gesproken taal) door een geautomatiseerd systeem om te zetten in geschreven tekst.
	12. Binnen de Nederlandse AI Coalitie ontstaat een samenwerkingsverband van bedrijven, overheden, semipublieke instellingen en kennisinstellingen die beogen samen te werken om spraakherkenning voor de Nederlandse taal verder te brengen. Een belangrijk onderdeel hiervan is het 'bijeenbrengen' van trainingsdata van verschillende bovengenoemde partijen. In hoeverre kunnen

	JenV organisaties voor het trainen van hun software gebruik maken van trainingsdata van zulke derde partijen? In hoeverre mogen derde partijen gebruik maken van trainingsdata van JenV organisaties voor het trainen van hun software? Hoe ligt dit wanneer het gaat om leveranciers van spraakherkenningssoftware? Gelden hier in juridische zin op grond van wet- en regelgeving nog andere beperkingen?
Afname uit de markt en samenwerking met bedrijven *Zijn er, los van kwalitatieve of economische overwegingen, in juridische zin beperkingen aan het gebruik van commerciële producten door JenV organisaties?*	13. Binnen Nederland wordt op het gebied van spraakherkenning en autotranscriptie ook samengewerkt tussen bedrijven, overheden, semipublieke instellingen en kennisinstellingen om deze technologie voor de Nederlandse taal verder te ontwikkelen. Een belangrijk onderdeel hiervan is het 'bijeenbrengen' van trainingsdata van verschillende bovengenoemde partijen. In hoeverre kunnen JenV-organisaties, voor het trainen van hun software, op een juridisch verantwoorde manier gebruik maken van trainingsdata van zulke derde partijen? In hoeverre mogen derde partijen gebruik maken van trainingsdata van JenV-organisaties voor het trainen van hun software? Hoe ligt dit wanneer het gaat om leveranciers van spraakherkenningssoftware? Gelden hier op grond van wet- en regelgeving nog andere beperkingen?
Overig	14. Welke vereisten c.q. beperkingen stellen de juridische kaders aan het gebruik van gespreksopnames, bijbehorende transcripties, metadata en op bovenstaande wijze geanonimiseerde trainingsdata voor wetenschappelijk onderzoek? Hoe kan aan die vereisten c.q. beperkingen worden voldaan door maatregelen in beleidsmatige of technische zin?
	15. Welke risico's kunnen zich voordoen t.a.v. publieke waarden van bescherming van persoonsgegevens, non-discriminatie en rechtsbescherming bij de inzet van spraakherkenning binnen het werkveld van justitie en veiligheid?
	16. Hoe kunnen die risico's worden gemitigeerd door maatregelen in beleidsmatige of technische zin?

	17. Mogen opnames van gesprekken die zijn gemaakt met als doel deze gesprekken te laten transcriberen (al dan niet door een geautomatiseerd systeem) ook gebruikt worden om personen in deze gesprekken te identificeren aan de hand van hun spraak (sprekerherkenning) voor opsporingsdoeleinden?

CONSIDERATI
LEGAL | PUBLIC AFFAIRS | RESPONSIBLE TECH

Technologie en data bieden kansen voor elke organisatie. De toepassing hiervan is voorpaginanieuws geworden. Maar deze vernieuwing wringt. Organisaties lopen tegen juridische vraagstukken en maatschappelijke belangen aan. En als organisatie wilt u hierin de regie behouden.

Considerati is het juridisch en public affairs adviesbureau voor de digitale wereld, met kantoren in Amsterdam en Den Haag. Wij helpen organisaties maatschappelijk verantwoord te innoveren met digitale technologie en data. Dit doen we met drie gespecialiseerde teams:

Legal: voor een datastrategie die compliant is met privacyregelgeving
Responsible Tech: voor een ethisch kompas bij innoveren met data en algoritme
Public Affairs: voor maatschappelijk en politiek draagvlak voor innovaties

En dit doen we al meer dan 15 jaar voor zowel grote bedrijven en overheden als groeiende organisaties.

Contact
Neem contact met ons op via **info@considerati** of bel naar 020 73 70 069. Voor meer informatie kunt u ook kijken op onze website via **www.considerati.nl**.