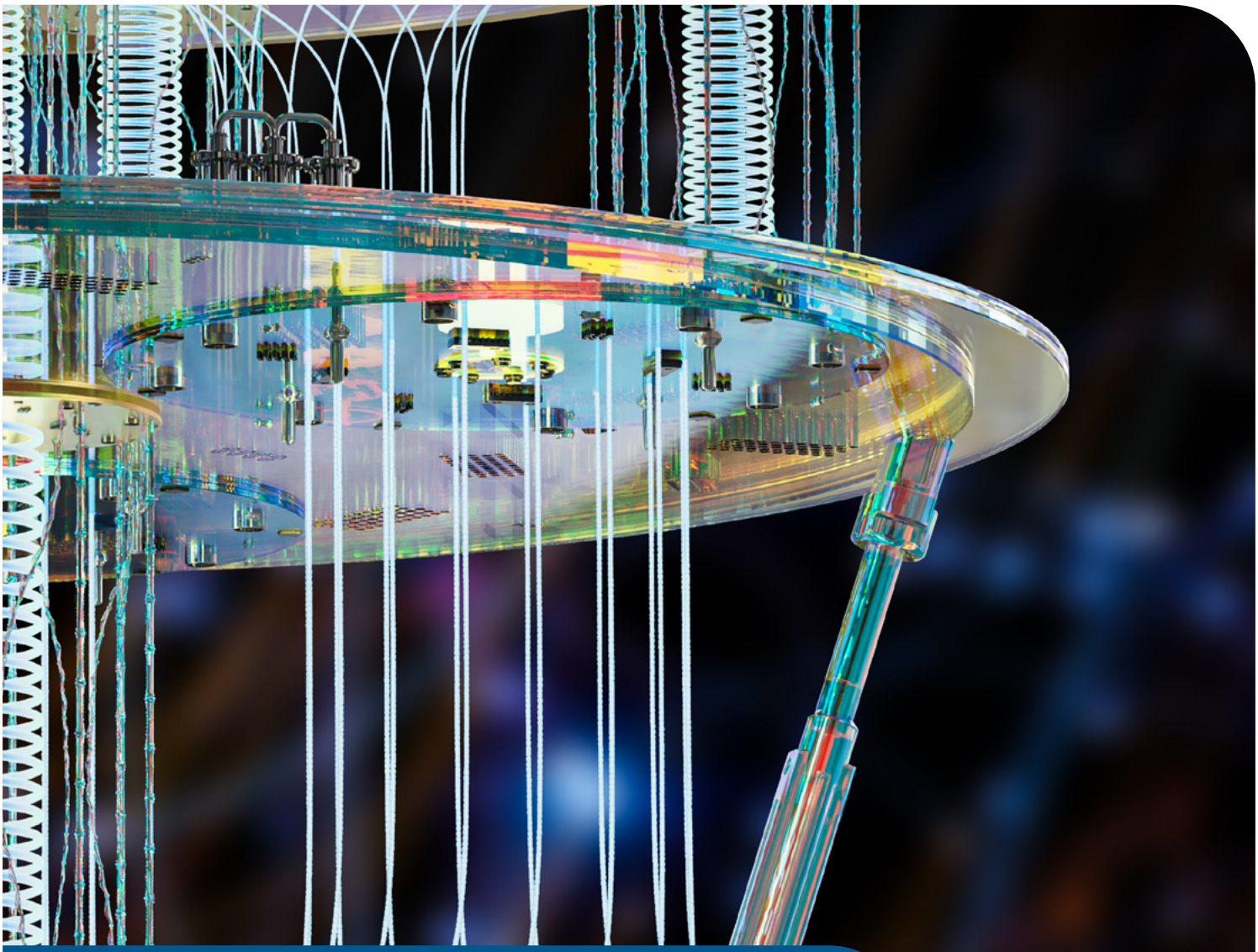
Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties



Quantumtechnologie in de maatschappij

Een verkenning van de implicaties voor publieke waarden en fundamentele rechten

QDNL

TU Delft

Universiteit van Amsterdam



Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties

Quantumtechnologie in de maatschappij

Een verkenning van de implicaties voor publieke waarden en fundamentele rechten







Voorwoord

Quantumtechnologie is volop in ontwikkeling en nieuwe toepassingen komen steeds duidelijker in beeld. Wat in eerste instantie misschien klinkt als een ingewikkeld onderwerp uit de natuurkunde, blijkt verrassend dichtbij te staan. Quantumtechnologie kan op termijn invloed hebben op de manier waarop we communiceren, medicijnen ontwikkelen of omgaan met onze digitale veiligheid. Daarmee kan de technologie raken aan vraagstukken die voor de samenleving van grote betekenis zijn.

Juist die mogelijke impact maakt quantumtechnologie voor mij meer dan alleen een technisch vraagstuk. Naarmate de technologie zich verder ontwikkelt, zullen keuzes moeten worden gemaakt over de manier waarop de technologie wordt toegepast en welke waarden daarbij worden meegenomen. Welke toepassingen vinden we wenselijk? Welke publieke waarden willen we beschermen? En hoe zorgen we ervoor dat de voordelen van deze technologie op een verantwoorde manier worden benut? Het zijn vragen die ik belangrijk vind om nu al te stellen.

Het tempo waarin de technologie zich zal ontwikkelen en de omvang van de maatschappelijke impact zijn weliswaar nog moeilijk te voorspellen, maar een paar jaar geleden leek ook generatieve AI nog vooral iets van de toekomst. Inmiddels is generatieve AI doorgedrongen tot ons dagelijks leven en beïnvloedt het de manier waarop we werken, leren en met informatie omgaan. Wat aanvankelijk ver weg lijkt, kan zich binnen enkele jaren ontwikkelen tot iets waar we allemaal mee te maken hebben.

Die ontwikkeling heeft voor mij duidelijk gemaakt hoe belangrijk het is om de maatschappelijke implicaties van een nieuwe technologie al in een vroeg stadium in beeld te brengen. Bij quantumtechnologie is daar nog ruimte voor. Omdat de technologie nog in ontwikkeling is, kunnen we vooruitkijken en maatschappelijke overwegingen meenemen voordat nieuwe toepassingen hun weg naar de samenleving vinden. Ik zie dat als een kans om stil te staan bij wat quantumtechnologie mogelijk kan maken en bij de manier waarop we deze technologie een plek willen geven in onze samenleving.

Vanuit die gedachte is dit rapport tot stand gekomen. Dit rapport laat zien hoe de ontwikkeling en toepassing van quantumtechnologie zich verhouden tot publieke waarden, zoals rechtvaardigheid, inclusie en democratische controle, en tot fundamentele rechten, zoals het recht op privéleven. Deze waarden en rechten bieden een kader om de keuzes die voor ons liggen zorgvuldig af te wegen.

Door in Nederland en Europa tijdig aandacht te hebben voor regelgeving, publieke betrokkenheid en passende waarborgen, kunnen we richting geven aan een technologie die aansluit bij onze waarden. Zo kan technologische vooruitgang hand in hand gaan met publieke waarden. Ik hoop dat dit rapport daaraan een bijdrage kan leveren.



Ik wens u veel leesplezier.

Gerdine Keijzer-Baldé

Kwartiermaker Directoraat-Generaal Digitaliseringsbeleid
Samenleving en Overheid (i.o.)
Ministerie van Economische Zaken en Klimaat

Over deze publicatie

Deze publicatie bestaat uit twee delen. Het eerste deel biedt een introductie op quantumtechnologie en verkent de mogelijke implicaties ervan voor publieke waarden, en fundamentele rechten. Daarbij staat *anticipatory governance*, ofwel anticiperend bestuur, centraal. Dit is een benadering die een vooruitziende blik vooropstelt bij beleid voor nieuwe, opkomende technologieën, zoals quantum, die vaak zijn omgeven met onzekerheid. Het doel van *anticipatory governance* is vat te krijgen op zulke onzekerheid en actie te ondernemen op het moment dat uitdagingen zich voordoen. Dit deel is geschreven door een onderzoeksteam van de TU Delft en Universiteit van Amsterdam dat betrokken is bij het Centre for Quantum and Society, onderdeel van QDNL.

Het tweede deel laat zien hoe quantumtechnologie in de praktijk wordt toegepast. Aan de hand van het *Exploratory Quantum Technology Assessment* (EQTA) wordt verkend welke maatschappelijke, ethische en juridische implicaties een concrete quantumtoepassing kan hebben. EQTA biedt een methodiek om deze implicaties vroegtijdig in kaart te brengen en de randvoorwaarden te identificeren die nodig zijn voor een verantwoorde ontwikkeling en toepassing van quantumtechnologie. Dit deel is opgesteld door het Centre for Quantum and Society.

Inhoud

Deel 1: Quantumtechnologieën, publieke waarden en fundamentele rechten **9**

Managementsamenvatting **11**

1. Inleiding **15**

2. Quantumtechnologie **17**

2.1. De basisbeginselen van quantummechanica 17

2.2. Quantumsensing 19

2.3. Quantumcomputing 20

2.4. Quantumcommunicatie 21

2.5. Samenhang tussen quantum- en klassieke digitale technologieën 22

2.6. Quantumtechnologieën op de korte en lange termijn 24

3. Publieke waarden in quantumtechnologieën: kansen en uitdagingen **27**

3.1. Definitie van waarden 27

3.2. Publieke waarden in quantumtechnologie 28

3.3. Kansen en uitdagingen voor publieke waarden 29

4. Quantumtechnologieën, recht en fundamentele rechten **42**

4.1. Wet- en regelgevingsinstrumenten 43

4.2. Quantumcomputing: communicatie- en informatieveiligheid 43

4.3. Quantumcomputing: fundamentele wetenschap, optimalisatie en machinelearning 46

4.4. Quantumsensing: privacy en gegevensbescherming 49

4.5. Waarborging van fundamentele rechten op de lange termijn 58

5. Aanbevelingen **60**

Deel 2: Quantumtechnologie in de praktijk **63**

Quantumtoepassingen en publieke waarden **65**

De EQTA-methodiek 65

Casus: OPM-MEG-helm met quantumsensoren in Amsterdam UMC 67

Handelingsopties 68

Colofon **71**

Deel 1:

Quantumtechnologieën, publieke waarden en fundamentele rechten

Managementsamenvatting

Het kraken van versleuteling en het mogelijk maken van ongekend nauwkeurige monitoring: het is nog toekomstmuziek, maar op de langere termijn kunnen quantumtechnologieën verstrekkende maatschappelijke gevolgen hebben. Dergelijke technologieën trekken daarom veel aandacht, hoewel ze zich nu nog een vroeg ontwikkelstadium bevinden. Welke quantumtechnologieën zijn er allemaal? En welke gevolgen kunnen ze hebben voor onze publieke waarden en de bescherming van onze fundamentele rechten? Dat komt aan de orde in dit deel.

Quantumtechnologie

Momenteel bevinden we ons aan het begin van de tweede generatie quantumtechnologieën. De eerste generatie maakte gebruik van bepaalde quantumechanische eigenschappen, wat heeft geleid tot toepassingen als halfgeleiders en lasers. De tweede generatie quantumtechnologieën benut quantumverschijnselen, zoals superpositie, verstrengeling en interferentie. Zo kunnen nieuwe, geavanceerde technologieën worden gecreëerd. Die technologieën zijn doorgaans in drie categorieën in te delen: quantumcomputing, quantumcommunicatie en quantumsensing. Quantumcomputing biedt mogelijkheden voor doorbraken op het gebied van farmacie en energieopslag. Tegelijkertijd brengt het ook bedreigingen met zich mee voor onder andere informatieveiligheid. Quantumcommunicatie biedt juist de belofte van nieuwe manieren om communicatie te beveiligen. Tot slot geldt quantumsensing op dit moment als het meest volwassen technologiegebied. Hierbij zijn er bijvoorbeeld toepassingen mogelijk op het gebied van navigatie en medische diagnostiek. Hoewel de potentie van quantumtechnologie groot is, is het belangrijk om te benadrukken dat veel toepassingen van quantumtechnologie nog niet verder komen dan de experimentele fase, met ontwikkeltrajecten die gekenmerkt worden door veel onzekerheid.

Publieke waarden in quantumtechnologieën: kansen en uitdagingen

Over het algemeen verwijzen waarden naar ideeën over wat ‘goed’ of ‘gewenst’ is, zoals menselijke autonomie, veiligheid, duurzaamheid of privacy. Ze helpen om te bepalen welke soorten doelen het waard zijn om na te streven. Publieke waarden drukken uit wat we als samenleving of groep belangrijk vinden. Bij de ontwikkeling en toepassing van opkomende technologieën, zoals quantum, moeten waarden worden meegewogen. Daarbij kan onderscheid

worden gemaakt tussen fundamentele waarden en technologiespecifieke waarden. Fundamentele waarden zijn bijvoorbeeld privacy, gelijkheid en inclusie. Voorbeelden van technologiespecifieke waarden zijn transparantie, verantwoordelijkheid en innovatie voor het algemeen belang. Op basis van literatuuronderzoek blijken in het bijzonder vijf publieke waarden van belang bij quantumtechnologieën: inclusie en participatie, privacy, rechtvaardigheid en menselijke integriteit, democratie en democratisering, openheid en open strategische autonomie.

Quantumtechnologieën bevinden zich zoals gezegd nog in een vroeg stadium van maatschappelijke toepassing. Daardoor kunnen bestuurlijke keuzes die nu worden gemaakt, deze publieke waarden in de toekomst versterken of juist ondermijnen. Aan de ene kant kunnen quantumtechnologieën bepaalde waarden versterken, bijvoorbeeld door veiligere communicatie-infrastructuren mogelijk te maken of door te ondersteunen bij besluitvorming. Aan de andere kant kunnen quantumtechnologieën ook risico's opleveren. Zo kunnen quantumtechnologieën participatie en inclusie beperken. Ook is het mogelijk dat enkele technologisch geavanceerde landen en bedrijven vroeg toegang krijgen tot quantumcapaciteiten, terwijl andere landen en bedrijven worden uitgesloten, wat kan leiden tot een wereldwijde *quantum divide*. Wanneer bij de ontwikkeling de nadruk ligt op strategische en veiligheidsperspectieven, kan dit mogelijk leiden tot een verschuiving van de besluitvorming naar gesloten, door experts aangestuurde domeinen. Dat roept zorgen op over democratisch toezicht en democratische openheid. Geopolitieke ontwikkelingen maken bovendien de verhouding tussen wetenschappelijke openheid en technologische soevereiniteit ingewikkelder. Landen proberen daar een balans te vinden tussen samenwerking en strategische autonomie. Deze inzichten laten zien dat de maatschappelijke impact van quantumtechnologieën sterk afhangt van hoe de ontwikkeling ervan wordt vormgegeven. Tijdige beleidskeuzes zijn van groot belang om innovatie en publieke waarden met elkaar in balans te brengen.

Quantumtechnologieën, recht en fundamentele rechten

Bestaande wettelijke kaders op Europees en nationaal niveau ondervangen vanwege hun technologieneutrale karakter de meeste uitdagingen op het gebied van fundamentele rechten en quantumtechnologieën. Maar uit literatuuronderzoek blijkt dat er ook aanvullende uitdagingen zijn.

Op het gebied van quantumcomputing ligt de belangrijkste uitdaging voor fundamentele rechten op het gebied van informatieveiligheid. Dit is essentieel voor de bescherming van het recht op (privé)communicatie en de bescherming van persoonsgegevens. Om deze uitdaging aan te pakken, wordt ingezet op post-quantum-cryptografie (PQC). Dit is een type versleuteling dat volgens experts niet gekraakt kan worden door toekomstige quantumcomputers. Meer in het algemeen worden informatiebeveiliging en de fundamentele rechten die door informatiebeveiliging worden geraakt, beschermd door bestaande wetgeving, waaronder de Algemene verordening gegevensbescherming (AVG) en richtlijnen op het gebied van cyberveiligheid (NIS2 en DORA). Deze regelgeving verplicht organisaties die eronder vallen om passende informatiebeveiligingsmaatregelen te treffen, die aansluiten bij de huidige stand van de techniek.

Een andere uitdaging voor quantumcomputing is de toegang ertoe. Zo kunnen er juridische problemen ontstaan bij het functioneren van intellectuele-eigendomsstelsels in het geval dat de markt gedomineerd zou worden door slechts één of enkele bedrijven. Er kunnen ook redenen zijn om de toegang tot quantumcomputing juist te bevorderen in het belang van wetenschap en innovatie. Die moeten afgewogen worden tegen redenen om potentieel misbruik te voorkomen. Exportcontroles en eisen voor kennisveiligheid kunnen daarnaast gevolgen hebben voor het uitoefenen van bepaalde fundamentele rechten van actoren in het quantuminnovatie-ecosysteem.

Quantumsensing kan ook voor uitdagingen zorgen, bijvoorbeeld op het gebied van privacy. Zo zouden organisaties quantumsensoren kunnen gebruiken om op afstand mensen of objecten te detecteren. Het gebruik van quantumsensingtechnologieën door burgers en bedrijven valt onder het recht op privéleven en bestaande wetgeving over gegevensbescherming. Het gebruik voor defensiedoeleinden valt buiten de reikwijdte van het EU-recht, maar kan wel worden onderzocht aan de hand van het Europees Verdrag voor de Rechten van de Mens. Dat vereist namelijk dat alle staatsinmenging met fundamentele rechten proportioneel en noodzakelijk is. Het is van groot belang dat bij de inzet van quantumtechnologieën rechtmatigheid, proportionaliteit en noodzaak streng beoordeeld worden. Ook is er meer aandacht nodig voor de wijze waarop bestaande en opkomende maatschappelijke, politieke en economische machtsverhoudingen de interactie tussen nieuwe technologieën en privacy vormgeven. Tegelijkertijd kunnen toepassingen van quantumsensing ook bijdragen aan de uitoefening van fundamentele rechten, bijvoorbeeld op het gebied van klimaat en milieu.

Tot slot benadrukt de analyse dat digitale soevereiniteit op zowel EU- als nationaal niveau een belangrijke factor is voor het vermogen van de overheid om de ontwikkeling van nieuwe technologieën te beïnvloeden, en sturing te geven aan de manier waarop quantumtechnologieën in de samenleving worden ingezet en uiteindelijk gevolgen kunnen hebben voor fundamentele rechten.

Aanbevelingen

Anticipatory governance, ofwel anticiperend bestuur,is een benadering die een vooruitziende blik centraal zet bij beleid voor nieuwe, opkomende technologieën. Dit kan bijdragen aan beleidsbeslissingen die zijn gebaseerd op waarden en die inspelen op vroege inzichten over quantumtechnologie. Zo kunnen beleidsmakers en besluitvormers snel en flexibel reageren op ontwikkelingen op zowel technologisch als beleidsgebied. Uit deze analyse volgen twee aanbevelingen:

1. Zorg voor continue, grondige monitoring van de ontwikkelingen op het gebied van quantumtechnologie.
2. Wees bereid om te handelen op basis van relevante publieke waarden en de mogelijke gevolgen voor fundamentele rechten.

1. Inleiding

Quantumtechnologieën bevinden zich nog in een zeer vroeg ontwikkelstadium. Toch trekken ze al veel aandacht vanwege hun mogelijke impact op uiteenlopende sectoren. Via QDNL investeert Nederland aanzienlijk in deze technologie. QDNL is het Nederlandse quantuminnovatie-ecosysteem waarin bedrijven, industrie, overheid en academici werken aan de ontwikkeling, opschaling en adoptie van quantumtechnologie om economische en maatschappelijke waarde te realiseren.

Hoewel quantumtechnologieën nog maar beperkt in de samenleving zijn doorgedrongen, kunnen ze potentieel verstrekkende gevolgen hebben, vooral op de wat langere termijn. Zo kunnen quantumcomputers in de toekomst mogelijk bestaande versleuteling kraken, wat voor veiligheidsrisico's zorgt. Ook is er onzekerheid over de invloed van quantumtechnologie op het milieu. Het is daarom belangrijk om mogelijke maatschappelijke gevolgen nu al in kaart te brengen. Dit kan door hier vanuit een lens van publieke waarden naar te kijken.[1] Waarden zijn ideeën over wat 'goed' of 'gewenst' is, bijvoorbeeld veiligheid, rechtvaardigheid of privacy. Ze helpen ons te bepalen welke doelen het waard zijn om na te streven. Publieke waarden drukken uit wat we als samenleving of groep belangrijk vinden.[2] Bij voorkeur worden publieke waarden al in een vroeg stadium geidentificeerd, zodat er ruimte is voor wetenschappers en beleidsmakers om hierop te anticiperen.[3] Daarnaast is het van belang om te onderzoeken hoe deze waarden beschermd worden door fundamentele rechten en relevante wetgeving.

Deze analyse biedt hiervoor een eerste aanzet. Het geeft een overzicht van quantumtechnologieën en relevante publieke waarden en fundamentele rechten, samen met een analyse van wet- en regelgevingsinstrumenten die deze waarden en rechten kunnen beschermen. De analyse is geschreven door een onderzoeksteam van de TU Delft en Universiteit van Amsterdam dat betrokken is bij het Centre for Quantum and Society, onderdeel van QDNL. Het is opgesteld op verzoek van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Er is ook samengewerkt met een stuurcommissie met leden van de Responsible Advancement of Quantum Technology (REAQT). Deze denktank wordt gevormd door TNO Vector, ECP | Platform voor de InformatieSamenleving, het Rathenau Instituut en het Centre for Quantum and Society.

1 Rathenau Instituut. (2023). *Quantumtechnologie in de samenleving*.

2 Rathenau Instituut. (2017). *Opwaarderen*.

3 Van Der Weij, F., et al. (2023). Value change and technological design. *IEEE Technology and Society Magazine*.

Leeswijzer

In hoofdstuk 2 komt de basis van quantumtechnologie aan de orde, en de drie relevante technologiedomeinen: quantumsensing, -computing en -communicatie. Ook gaat het hoofdstuk in op enkele belangrijke risico's op de korte en lange termijn. Hoofdstuk 3 brengt de publieke waarden in kaart die relevant zijn voor quantumtechnologieën. Hoofdstuk 4 analyseert de relevante kaders voor quantumtechnologieën op het gebied van regelgeving en fundamentele rechten. Hoofdstuk 3 heeft dus een ethisch perspectief en hoofdstuk 4 een juridisch perspectief. Deze perspectieven vormen samen elementen van *anticipatory governance*, ofwel anticiperend bestuur.[4] *Anticipatory governance* zet een vooruitziende blik centraal bij beleid voor nieuwe, opkomende technologieën, zoals quantum. Dergelijke nieuwe technologieën zijn vaak omgeven met onzekerheid. Het doel van anticiperend bestuur is vat te krijgen op zulke onzekerheid en actie te ondernemen op het moment dat uitdagingen zich voordoen. Tot slot geeft hoofdstuk 5 een overzicht van de aanbevelingen voor beleidsmakers.

4 Organisatie voor Economische Samenwerking en Ontwikkeling. [OESO]. (2024). Framework for anticipatory governance of emerging technologies. *OECD Science, Technology and Industry Policy Papers*.

2. Quantumtechnologie

Diverse bestaande technologieën zijn al gebaseerd op de beginselen van quantummechanica. Denk aan halfgeleiders, lasers en MRI-scanners. Dit soort technologieën worden soms ‘eerste generatie quantumtechnologieën’ genoemd. Ze zijn gebaseerd op de grondregels van de quantumfysica, maar maken niet actief gebruik van quantumeffecten.[5] Deze technologieën vormen het fundament voor de huidige digitale infrastructuur, van computers en smartphones tot het internet.

Tweede generatie quantumtechnologieën gaan een stap verder: hierbij worden geavanceerde quantummechanische eigenschappen ontworpen om taken op het gebied van informatieverwerking, communicatie en nauwkeurige metingen uit te voeren die met de klassieke natuurkunde niet kunnen worden gereproduceerd.[6] Quantumtechnologieën van de tweede generatie benutten de eigenschappen van quantummechanica om nieuwe manieren van informatieverzameling, -verzending en -verwerking makkelijker te maken. Deze technologieën passen in drie hoofdgebieden: quantumsensing, quantumcomputing en quantumcommunicatie.

Om een goed beeld te krijgen van de mogelijkheden van quantumtechnologieën, geeft dit hoofdstuk uitleg over enkele belangrijke kernconcepten en begrippen. Paragraaf 2.1 geeft een overzicht van de basisbeginselen van quantummechanica. Paragraaf 2.2, 2.3 en 2.4 gaan achtereenvolgens in op quantumsensing, quantumcomputing en quantumcommunicatie. Vervolgens bespreekt paragraaf 2.5 de samenhang tussen quantum- en klassieke digitale technologieën. Tot slot gaat paragraaf 2.6 in op de mogelijke ontwikkeling van quantumtechnologieën op de korte en lange termijn.

2.1. De basisbeginselen van quantummechanica

Quantummechanica is een natuurkundige theorie die beschrijft hoe de natuur zich gedraagt in hele kleine deeltjes, zoals elektronen en fotonen, atomen en moleculen. Op het niveau van deze hele kleine deeltjes is het gedrag van systemen erg verschillend van het ‘klassieke’ gedrag dat mensen kennen uit hun dagelijkse ervaringen.[7]

5 Dowling, J. & Milburn, G. (2002). *Quantum Technology: The Second Quantum Revolution*. Philosophical Transactions of the Royal Society A.
6 OESO. (2024). Framework for Anticipatory Governance of Emerging Technologies. *OECD Science, Technology and Industry Policy Papers*.
7 Griffiths, D. J., & Schroeter, D. F. (2018). *Introduction to Quantum Mechanics* (3e editie). Cambridge University Press.

Superpositie, verstrengeling en interferentie zijn drie eigenschappen van de quantummechanica die belangrijk zijn voor quantumtechnologieën.[8]

Superpositie

In tegenstelling tot bits van klassieke systemen, die uitsluitend de waarde 0 of 1 kunnen aannemen, kan een qubit zich in een superpositie van beide toestanden tegelijk bevinden.[9] Een qubit kan dus zowel 0 als 1 zijn. Wanneer een qubit wordt gemeten, stort deze superpositie in tot één bepaalde waarde, waarbij de uitkomst wordt bepaald door waarschijnlijkheden. Deze informatie is niet rechtstreeks toegankelijk en kan alleen worden verkregen door het quantumsysteem herhaaldelijk opnieuw te creëren, vervolgens te meten en de statistieken van die metingen te analyseren. Deze statistische willekeurigheid is een fundamenteel kenmerk van quantumsystemen. Quantumtechnologieën en quantumalgoritmen kunnen deze amplitudes benutten om veel bewerkingen tegelijk uit te voeren en subtiele fysieke signalen te versterken. Daardoor kunnen zij, voor bepaalde soorten problemen, reken- en meetprestaties leveren die de prestaties van klassieke computers en sensoren ruimschoots overtreffen.[10]

Verstrengeling

Verstrengeling creëert krachtige verbanden tussen twee of meer quantumsystemen, op een manier dat ze zich als één onscheidbare entiteit gedragen. Dit betekent dat het meten van het ene systeem onmiddelijke invloed heeft op de toestand van het andere systeem, zelfs op grote afstand. Klassieke ICT-systemen kunnen deze effecten niet reproduceren. Verstrengeling vormt de basis voor verschillende quantumtechnologieën, waaronder veilige communicatieprotocollen, het meten met grote precisie en multi-qubitoperaties in het kader van quantumcomputing.[11]

Interferentie

Quantumtoestanden gedragen zich als golven en als deeltjes. Als ze elkaar overlappen, kunnen ze elkaar versterken of uitdoven, wat leidt tot een effect dat interferentie wordt genoemd.[12] Quantumtechnologieën gebruiken interferentie om de gewenste resultaten van een berekening of meting te versterken en ongewenste resultaten te onderdrukken. Bij quantumcomputing wordt interferentie gebruikt voor het ontwerpen van algoritmen die de waarschijnlijkheid van

8 OESO. (2024). Framework for Anticipatory Governance of Emerging Technologies. *OECD Science, Technology and Industry Policy Papers*.
9 Ibid.
10 Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.
11 OESO. (2024). Framework for Anticipatory Governance of Emerging Technologies. *OECD Science, Technology and Industry Policy Papers*.
12 Ibid.

superpositie naar de gewenste oplossing sturen. Bij quantumsensing maken interferentiepatronen metingen mogelijk op een schaal en met een precisie die niet mogelijk is met klassieke apparaten.

2.2. Quantumsensing

Quantumsensoren zijn een nieuw type sensortechnologie. Ze gebruiken de quantumeigenschappen superpositie, verstrengeling en coherentie (dit is gerelateerd aan interferentie) om heel nauwkeurig signalen te meten, zoals zwaartekracht, druk en magnetische velden. Een aantal toepassingen van sensoren die quantumeffecten gebruiken bestaan al. Zo zijn *magnetic resonance imaging* (MRI), atoomklokken en gps het gevolg van ontdekkingen tijdens de eerste quantumrevolutie. Bovendien wordt quantumsensing al deels commercieel toegepast, bijvoorbeeld voor medische beeldvorming. De meeste ontwikkelingen in dit quantumdomein bevinden zich echter nog in de onderzoeks- en ontwikkelingsfase, met onzekerheid over hoe en waar de toepassing ervan zal plaatsvinden.[13]

Een van de mogelijke toekomstige toepassingen van quantumsensing is in het medische domein, zoals in onderzoek, diagnose en ziektepreventie.[14] Quantumsensoren maken met ongekend detail niet-invasieve, real-time monitoring mogelijk van de hersenen, en ook van neurologische- en hartactiviteit.[15] Deze toepassing bevindt zich al in een vergevorderd stadium en is gebaseerd op NV-centra. Dit staat voor *nitrogren-vacancy-centres*. Hierbij worden defecten in de structuur van diamanten gebruikt om magnetische velden op nanoschaal te meten.[16] Andere mogelijke biomedische toepassingen maken gebruik van *superconducting quantum interference devices* (SQUIDs). Deze SQUIDs maken niet-invasieve monitoring mogelijk van magnetische velden in de hersenen. Ook atomaire dampen, die bijvoorbeeld worden toegepast in systemen voor magneto-encefalografie (MEG), kunnen hersensignalen detecteren die zich dieper in de hersenen bevinden.[17]

Quantumsensingtoepassingen kunnen ook meerwaarde bieden voor nauwkeurige navigatie en tijdsbepaling. Denk aan compacte optische klokken en atoominterferentiemeters.[18] Quantumsensing biedt daarmee veel kansen voor defensie, omdat quantumsensing traditionele militaire toepassingen kan verbeteren, zoals accurate positiebepaling, (traagheids)navigatie en

13 Bongs, K., et al. (2023). Quantum sensors will start a revolution – if we deploy them right. *Nature*.

14 Aslam, N., et al. (2023). Quantum sensors for biomedical applications. *Nature Reviews Physics*.

15 Fairbairn, R., et al. (2025). *Emerging applications of quantum sensing technology in healthcare*. NIHR Innovation Observatory.
Taylor, M. A. & Bowen, W. P. (2016). Quantum metrology and its application in biology. *Physics Reports*.

16 Debuisschert, T. (2021). Quantum sensing with nitrogen-vacancy colour centers in diamond. *Photoniques*.

17 Ibid.

18 Alonso, I., et al. (2022). Cold atoms in space: Community workshop summary and proposed road-map. *EPJ Quantum Technology*.

Positioning, Navigation and Timing (PNT).[19] Deze toepassingen kunnen navigatie mogelijk maken in omgevingen zonder gps, of ervoor zorgen dat navigatie niet afhankelijk is van gps dat kwetsbaar is voor signaalverstoring (*jamming*) of signaalvervalsing (*spoofing*).[20]

Naast het medische en militaire domein, zijn er ook nog andere toepassingen van quantumsensoren. Zo kunnen *cold atom interferometers* vulkaanuitbarstingen of aardbevingen meten. Ze wegen echter meer dan 100 kilo, wat ze lastig te gebruiken maakt in de praktijk. De al genoemde NV-centra zijn aanzienlijk kleiner en lichter dan *cold atom interferometers* en kunnen ook worden gebruikt voor het in kaart brengen van veranderingen in het magnetische veld van de aarde.[21] Het meten van kleine variaties in zwaartekrachtvelden of bodembeweging[22] kan zeer waardevol zijn voor bijvoorbeeld mijn- en grondstoffenexploratie en voor het monitoren van infrastructuur.

2.3. Quantumcomputing

Quantumcomputing is gebaseerd op qubits die quantummechanische beginselen gebruiken voor het verwerken van informatie.[23] Quantumcomputing maakt het mogelijk bepaalde problemen efficiënter op te lossen dan met klassieke computers en algoritmen.[24] Een bekend voorbeeld is het algoritme van Shor voor het vinden van de priemfactoren van grote getallen. Veel versleuteling is tegenwoordig gebaseerd op ontbinding van een heel getal in priemfactoren. Ontbinden is voor mensen en klassieke computers lastig als de getallen groot worden. Daardoor zijn data goed beveiligd. Volgens het algoritme van Shor kan een voldoende krachtige quantumcomputer grote getallen efficiënt ontbinden in factoren. Dit algoritme vormt daarmee een directe bedreiging voor huidige versleutelingsmethoden.[25] Het algoritme van Grover illustreert daarnaast een ander probleem dat quantumcomputing makkelijker kan oplossen.

---

19 European Commission, Directorate-General for Defense Industry and Space. (2025). *Quantum technologies in defence*. Publications Office of the European Union.

20 El-Sheimy, N., & Youssef, A. (2020). Inertial sensors technologies for navigation applications: State of the art and future trends. *Satellite Navigation*.

21 Blom, T., et al. (2023). *Radio en navigatie met behulp van kwantumsensoren. Toepassingen en impact op het frequentiespectrum.* Dialogic & TNO.

22 Stray, B., et al. (2022). Quantum sensing for gravity cartography. *Nature*.

23 Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.

24 Denk bijvoorbeeld aan problemen met gecombineerde optimalisatie, simulatie van quantumsystemen, of patroonextracties in ruimten met een hoge dimensionaliteit. Zie de volgende publicaties voor meer informatie:

Farhi, E., et al. (2014). A Quantum Approximate Optimization Algorithm. *arXiv*.

Georgescu, I. M., et al. (2014). Quantum simulation. *Reviews of Modern Physics*.

Biamonte, J., et al. (2017). Quantum machine learning. *Nature*.

25 Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*.

Dit algoritme verwijst naar een quantumtechniek die het doorzoeken van ongestructureerde data versnelt, doordat het aantal benodigde bewerkingen afneemt.[26]

Op de korte termijn is het simuleren van quantumfysicasystemen waarschijnlijk de veelbelovendste toepassing van quantumcomputers. Dit kan worden ingezet in veel verschillende sectoren. Zo kunnen in de scheikunde en materiaalwetenschap bijvoorbeeld moleculaire systemen gesimuleerd worden.[27] Dit kan leiden tot wetenschappelijke doorbraken op het gebied van farmacie, energieopslag, meststoffen en duurzame productie. In de logistiek,[28] telecommunicatie en financiën kunnen quantumcomputers en -algoritmen mogelijk verbetering brengen in routing, planning, optimalisatie van portfolio's en het in kaart brengen van risico's. In de energiebranche zou het simuleren van quantumfysicasystemen kunnen leiden tot nieuwe chemische stoffen voor batterijen of de optimalisatie van elektriciteitsnetten.[29]

2.4. Quantumcommunicatie

Quantumcommunicatie gebruikt de eigenschappen van quantummechanica om nieuwe vormen van veilige informatie-uitwisseling mogelijk te maken en, op de langere termijn, het creëeren van netwerken van quantumcomputers. Klassieke communicatiesystemen verzenden informatie door bits te coderen in lichtdeeltjes (fotonen), terwijl quantumcommunicatie is gebaseerd op de transmissie van qubits. Hierbij coderen de quantumtoestanden de informatie.[30] Quantumcommunicatie maakt gebruik van verstrengeling.[31] Door verstrengelde fotonen te distribueren tussen knooppunten, wordt het mogelijk een quantumnetwerk, en vervolgens een quantuminternet te bouwen. Daarin kan quantuminformatie worden verzonden, verwerkt en gedeeld tussen apparaten die zich op afstand van elkaar bevinden.[32] Een dergelijk netwerk vereist over het algemeen tussenstations (*quantumrepeaters*) die in een keten over lange

26 De versnelling die het algoritme van Grover biedt, is minder groot. Zie ook: Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In G. L. Miller (Red.), *STOC '96: Proceedings of the 28th ACM Symposium on Theory of Computing* (pp. 212-219). Association for Computing Machinery.

27 Cao, Y., et al. (2019). Quantum chemistry in the age of quantum computing. *Chemical Reviews*.

McArdle, S., et al. (2020). Quantum computational chemistry. *Reviews of Modern Physics*.

28 European Commission, Directorate-General for Defense Industry and Space. (2025). *Quantum technologies in defence*. Publications Office of the European Union.

Taylor, M. A. & Bowen, W. P. (2016). Quantum metrology and its application in biology. *Physics Reports*.

29 Peruzzo, A., et al. (2014). A variational eigenvalue solver on a photonic quantum processor. *Nature Communications*.

30 Gisin, N., et al. (2002). Quantum cryptography. *Reviews of Modern Physics*.

31 Kimble, H. J. (2008). The quantum internet. *Nature*.

Vermaas, P., et al. (2019). *Quantum internet: The internet's next big step*. TU Delft.

32 Ibid.

afstanden verstrengeling creëren en distribueren.[33] Naar verwachting zullen satellieten een belangrijke rol spelen in toekomstige grootschalige quantumnetwerken, omdat quantumsignalen in de ruimte minder last hebben van verlies en interferentie dan in glasvezelnetwerken.[34]

Een andere mogelijk veelbelovende toepassing van quantumcommunicatie is netwerkbeveiliging. Quantuminformatie kan niet worden gekopieerd zonder de oorspronkelijke toestand te veranderen.[35] Daardoor kan een afluisteraar quantumsignalen niet onderscheppen zonder daarbij sporen achter te laten. Het eerste protocol voor *quantum key distribution* (QKD) was gebaseerd op deze principes en werd in 1984 geconceptualiseerd. QKD stelt twee partijen in staat om veilige gedeelde encryptiesleutels te genereren.[36] Er zijn inmiddels verschillende succesvolle voorbeelden die op korte termijn kunnen leiden tot concrete toepassingen in specifieke situaties.[37]

2.5. Samenhang tussen quantum- en klassieke digitale technologieën

De ontwikkeling van quantumtechnologieën kan niet los worden gezien van andere digitale technologieën. Dat komt doordat ze de bestaande digitale infrastructuur waarschijnlijk niet vervangen, maar juist aanvullen.[38] Veel technieken werden oorspronkelijk gepresenteerd als doorbraken in quantumcomputing. Deze technieken bleken echter ook te werken op klassieke computers als werd voldaan aan vergelijkbare aannames over toegang tot data of onderliggende wiskundige structuren.[39] Hieruit blijkt dat quantumonderzoek waardevol kan zijn, zelfs als de hardware voor schaalbare quantumcomputing nog ontbreekt.

Het opkomende veld van *quantum-machinelearning* (QML) onderzoekt bijvoorbeeld hoe quantumalgoritmen traditionele taken voor *machinelearning* kunnen verbeteren. QML toont het potentieel van de combinatie tussen quantum- en klassieke technieken.[40] Denk aan een aanbevelingsalgoritme dat is gebaseerd op klassieke technieken. Onderzoekers hebben aangetoond dat zo'n algoritme vergelijkbare resultaten kan bereiken als het op een

33 Briegel, H. J., et al. (1998). Quantum repeaters: The role of imperfect local operations in quantum communication. *Physical Review Letters*.
34 Liao, S.-K., et al. (2017). Satellite-to-ground quantum key distribution. *Nature*.
35 Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*.
36 Pirandola, S., et al. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*.
37 Yin, J., et al. (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science*.
Zie ook voor een korte bespreking van QKD en informatiebeveiliging: OESO. (2025). A quantum technologies policy primer. *OECD Digital Economy Papers*.
38 OESO. (2025). A quantum technologies policy primer. *OECD Digital Economy Papers*.
39 Arrazola, J. M., et al. (2019). Quantum-inspired algorithms in practice. *arXiv*.
40 Biamonte, J., et al. (2017). Quantum machine learning. *Nature*.

quantumalgoritme is gebaseerd, zonder dat er quantumhardware voor nodig is.[41] Daarnaast zijn er lineaire algebratechnieken die hun inspiratie halen uit quantumalgoritmen. Die prestaties zijn vergelijkbaar en soms zelfs beter dan bestaande methoden met grote datasets.[42]

Het Open Quantum Institute (OQI) liet in 2024 al zien welke mogelijkheden er kunnen ontstaan door klassieke en quantumtechnieken te combineren voor het aanpakken van klimaatuitdagingen.[43] Een van die mogelijkheden is de toepassing van *quantum generative adversarial networks* (QGANs) voor de ontwikkeling van nieuwe chemische katalysatoren en materialen die kunnen bijdragen aan CO_2-afvang en de vermindering van CO_2-uitstoot. Hoewel deze toepassingen zich grotendeels nog in de verkennende fase bevinden, laten zij zien dat de verdere ontwikkeling van quantumtechnologie in combinatie met klassieke methoden krachtige nieuwe mogelijkheden kan bieden om complexe maatschappelijke uitdagingen aan te pakken.[44]

Op een fundamenteler niveau blijkt dat een groot deel van de huidige kracht van quantumalgortimen gebaseerd is op bewerkingen die ook in de klassieke informatica bekend zijn. Veel invloedrijke quantumalgoritmen zijn gebaseerd op transformatiematrices, maar dat geldt ook voor klassieke methoden voor data-analyse, optimalisatie en *machinelearning*.[45] Dit suggereert dat quantumcomputing bestaande algoritmische benaderingen vooral verfijnt en uitbreidt, in plaats van dat het een geheel nieuw paradigma vormt. Daarom stellen sommige onderzoekers dat de term *quantum advantage* minder geschikt is om uitsluitend te gebruiken bij ontwikkelingen in quantumtechnologie. Het gaat namelijk niet om vooruitgang die alleen toe te schrijven is aan quantumtechnologie, maar om vooruitgang dankzij de wisselwerking tussen quantum-, klassieke en hybride methoden.[46]

---

41 Tang, E. (2018). A quantum-inspired classical algorithm for recommendation systems. *arXiv*.

42 Arrazola, J. M., et al. (2019). Quantum-inspired algorithms in practice. *arXiv*.

43 Open Quantum Institute. (2024). *White Paper 2024. SDG Use cases.*

44 Een quantumextensie van een traditioneel ***generative adversarial network*** (GAN), een *machinelearning*-techniek waarbij twee modellen met elkaar concurreren om realistische data te produceren en te beoordelen. Op dit moment staan 'klassieke' GANs aan de basis van belangrijke vooruitgang in onder andere beeldgeneratie, geneesmiddelenonderzoek en materiaalontwerp. Hun quantum-tegenhangers (QGANs) breiden dit idee uit door quantumcircuits te gebruiken om complexe patronen te verkennen. Ze zijn echter nog vooral experimenteel, omdat implementaties momenteel kleinschalige ***proof-of-concept***-experimenten zijn die worden beperkt door het beperkte aantal qubits en de ruis in bestaande hardware. Pajuhanfard, M., et al. (2025). Quantum generative adversarial network for image generation. *The Visual Computer*.

45 Gilyén, A., et al. (2019). Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics. In M. Charikar (Red.), *STOC 2019: Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing* (pp. 193–204). Association for Computing Machinery.

46 Schuld, M., & Killoran, N. (2022). Is quantum advantage the right goal for quantum machine learning? *PRX Quantum*.

2.6. Quantumtechnologieën op de korte en lange termijn

Quantumsensing

Quantumsensing is het verst gevorderd van de besproken quantumtechnologieën. Sommige soorten quantumsensoren vinden langzaam hun weg naar de commerciële markt. Vanuit technisch oogpunt blijkt het echter lastig om quantumsensoren uit de laboratoriumfase te krijgen en breder toe te passen.[47] Veel quantumsensoren functioneren namelijk relatief goed in een laboratorium, maar daarbuiten verslechteren soms de prestaties. Dit komt door een paradox in de quantumfysica: hoe nauwkeuriger je iets wilt meten, hoe gemakkelijker dit wordt verstoord door andere (omgevings)factoren. De uitdaging voor quantumsensoren is om deze verstoring te beheersen.

Om quantumsensoren daadwerkelijk commercieel in te kunnen zetten, zijn ook andere factoren relevant. Daarbij spelen de mate waarin zij voorzien in een specifieke behoefte, hun prestaties en de zogenoemde SWaP-C-score een rol. Dit staat voor de *size* (S), *weight* (W), *power* (P) en *cost* (C) van sensoren. Quantumsensoren zijn duur. Daarom voorspellen analisten dat innovaties in het civiele domein, zoals op het gebied van telecommunicatie, waarschijnlijk eerder tot stand zullen komen door andere technologieën. Dit komt doordat quantumsensoren niet goed genoeg presteren om te kunnen concurreren met klassieke sensoren.[48] Elders zullen quantumsensoren waarschijnlijk wel ingezet worden. Zo is defensie koploper in het gebruik van quantumsensingtechnologieën.[49] Zoals al is benoemd in paragraaf 2.2, is een ander voordeel dat quantumsensing kan zorgen voor betere toepassingen op het gebied van navigatie en plaats- en tijdsbepaling.

Quantumcomputing

Er is de afgelopen jaren veel vooruitgang geboekt op het gebied van quantumcomputing. Toch is het nog onduidelijk wanneer quantumcomputing breder commercieel beschikbaar en relevant zal worden.[50] Het is namelijk lastig om quantumcomputing verder te verbeteren en op te schalen.[51] Hoewel er al meerdere prototypes bestaan, kan het nog geruime tijd duren voordat quantumcomputers groot en stabiel genoeg zijn om berekeningen uit te voeren die klassieke

47 Bongs, K., et al. (2023). Quantum sensors will start a revolution – if we deploy them right. *Nature*.

48 Rathenau Instituut. (2023). *Quantumtechnologie in de samenleving*.

49 Tucker, P. (2025, 18 november). Can Quantum Sensing Improve Magnetic Navigation? Pentagon Thinks One Company Is on the Right Track. *Defense One*.

50 Groenland, K. (2025). *Introduction to Quantum Computing for Business*. Amsterdam University Press.

51 Top, N. (2024). Preparing for a future with responsible quantum technologies. *Understanding quantum technologies through a lens of responsible tech*. SURF.

computers niet aankunnen.[52] Ondanks de beperkingen vormen quantumcomputers al een aanzienlijk risico voor de huidige versleutelingsmethoden waarmee de meeste digitale communicatie beveiligd is. Dit heeft de zoektocht naar quantumbestendige oplossingen versneld, zoals post-quantum-cryptografie (PQC). PQC maakt gebruik van nieuwe methoden die bestand zijn tegen bekende quantumaanvallen.[53]

Quantum-cloudcomputing (QCC) is een andere ontwikkeling. QCC is een nieuw cloudgebaseerd model dat moet zorgen voor een makkelijkere toegang tot quantumcomputing voor het brede publiek.[54] Bedrijven als Amazon, Microsoft en IBM zijn inmiddels begonnen met het aanbieden van dergelijke quantumdiensten.

Quantumcommunicatie

Quantumcommunicatie verkeert nog in een vroeg stadium. Er bestaat daarom grote onzekerheid over wanneer grootschalige quantumnetwerken beschikbaar zullen komen. Het verzenden van qubits over lange afstanden is een grote uitdaging.[55] De afhankelijkheid van hardware die zich nog in een vroege ontwikkelfase bevindt, zoals fotondetectoren en *quantumrepeaters*, maakt de technologie kwetsbaar en gevoelig voor operationele beperkingen. Hierdoor blijven huidige toepassingen buiten het laboratorium voorlopig nog beperkt tot netwerken van zogenoemde *trusted repeaters*.[56] Dat maakt quantumcommunicatie gevoelig voor operationele kwetsbaarheden, zoals instabiliteit, gaten in de beveiliging en specifieke oplossingen per leverancier.[57] Dat laatste zorgt ook voor beperkte interoperabiliteit tussen systemen. Dit vergroot het risico op fragmentatie en kan het opschalen of verbinden van quantumnetwerken tusen organisaties of landen bemoeilijken.[58]

52 Vermaas, P., & Mans, U. (2024). *Quantum Technologies and their Global Impact*. QDNL.

53 OESO. (2024). Framework for Anticipatory Governance of Emerging Technologies. *OECD Science, Technology and Industry Policy Papers*. Zie ook paragraaf 4.4.

54 Golec, M., et al. (2024). Quantum cloud computing: Trends and challenges. *Journal of Economy and Technology*.

55 Wehner, S., et al. (2018). Quantum internet: A vision for the road ahead. *Science*.

56 Scarani, V., et al. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*.

57 Biamonte, J., et al. (2017). Quantum machine learning. *Nature*.

58 European Telecommunications Standards Institute. (2021). *Quantum Key Distribution (QKD); Control and management interfaces* (ETSI GS QKD 015 V1.1.1 (2021-03)).

In de praktijk betekent dit dat quantumcommunicatie systemen lastig stabiel en voorspelbaar te gebruiken zijn. Ervaringen laten zien dat dergelijke systemen regelmatig moeten worden gekalibreerd en afhankelijk zijn van zorgvuldig gecontroleerde omgevingscondities.[59] Een quantumbeveiligde verbinding kan daardoor in theorie sterke beveiligingsgaranties bieden, maar in de praktijk slechts wisselende prestaties leveren en veel middelen vragen voor beheer en onderhoud.

Tegelijkertijd zijn huidige implementaties doorgaans gebaseerd op zogeheten *trusted-node*-architecturen. Hierdoor is de beveiliging afhankelijk van quantumprotocollen, en van de fysieke, digitale en operationele beveiliging van tussenliggende knooppunten. Wanneer een dergelijk knooppunt wordt aangetast, bijvoorbeeld door een cyberaanval of kwetsbaarheden in de toeleveringsketen, kunnen beveiligingsgaranties ook worden verzwakt.[60]

59 Biamonte, J., et al. (2017). Quantum machine learning. *Nature*.

60 Bongs, K., et al. (2023). Quantum sensors will start a revolution – if we deploy them right. *Nature*.

3. Publieke waarden in quantumtechnologieën: kansen en uitdagingen

3.1. Definitie van waarden

Over het algemeen verwijzen waarden naar ideeën van wat 'goed' of 'gewenst' is, zoals menselijke autonomie, veiligheid, duurzaamheid of privacy. Ze helpen ons te beslissen welke doelen het waard zijn om na te streven. Publieke waarden drukken uit wat we als samenleving of groep belangrijk vinden.[61] Waarden moeten daarom worden onderscheiden van de voorkeuren of belangen van individuen. Waarden zijn overtuigingen of principes waarvan mensen vinden dat ze in het algemeen moeten worden nagestreefd om een goed leven te leiden of een rechtvaardige maatschappij te realiseren.[62] De strijdkreet van de Franse revolutie, 'vrijheid, gelijkheid en broederschap', drukte bijvoorbeeld waarden uit die werden gezien als waarden die iedereen belangrijk vond.

De samenhang tussen technologie en maatschappij wordt vaak besproken in de context van waarden.[63] Waarden zijn niet statisch; ze veranderen in de loop van de tijd en kunnen meer of minder relevant worden.[64] Zo wordt duurzaamheid tegenwoordig steeds vaker meegenomen als een waarde bij het ontwerp van nieuwe technologieën. Dit was echter niet altijd een relevante waarde; ze kwam pas op tijdens de energietransitie. Een ander voorbeeld is het besef dat windturbines voor geluidsoverlast kunnen zorgen, waar mensen die er in de buurt wonen veel last van kunnen hebben. Dit inzicht leidde tot het opnemen van (geestelijke) gezondheid als waarde bij het ontwerp van windturbines. De integratie van waarden met technologie – en de reflectie daarop – staat centraal bij het vormgeven van inclusieve en verantwoorde technologische innovatie.

61 Rathenau Instituut. (2017). *Opwaarderen*.

62 Van de Poel, I. & Royakkers, L. (2011). *Ethics, Technology and Engineering: An Introduction* (p. 47). Wiley-Blackwell.

63 Swierstra, T., et al. (2009). Exploring techno-moral change: the case of the obesity pill. In P. Sollie & M. Düwell (Reds.), *Evaluating New Technologies: Methodological Problems for the Ethical Assessment of Technology Developments.* (pp. 119-138). Springer Netherlands.

64 Rathenau Instituut. (2023). *Quantum Technology in Society*.

Bij de governance van opkomende technologieën kunnen waarden worden ingedeeld in fundamentele en technologiespecifieke waarden.[65] Volgens de Organisatie voor Economische Ontwikkeling en Samenwerking (OESO) zijn fundamentele waarden 'gedeelde verbintenissen aan idealen van ethisch, politiek, economisch of cultureel belang – ongeacht of ze individueel, maatschappelijk, professioneel of institutioneel zijn of van een gemeenschap of natie'.[66] Zo kan privacy relevant worden als fundamentele waarde wanneer nieuwe technologieën invloed hebben op de bescherming van persoonsgegevens. Andere voorbeelden van fundamentele waarden zijn onder andere gelijkheid en inclusie. Naast de fundamentele waarden zijn er ook technologiespecieke waarden. Die kunnen dienen als een leidraad voor beleidsbeslissingen. Deze waarden bieden 'een morele en politieke basis voor de prioriteiten en compromissen die kenmerkend zijn voor alle governancebeslissingen op technologisch gebied'.[67] De OESO noemt als voorbeelden onder andere betrouwbaarheid, verantwoordelijkheid, transparantie en innovatie voor het algemeen belang. Fundamentele en technologiespecifieke waarden kunnen niet los van elkaar worden gezien en het is daarom essentieel dat deze waarden in samenhang worden bekeken.

3.2. Publieke waarden in quantumtechnologie

Hoewel quantumtechnologieën tot nu toe nog niet ver zijn doorgedrongen in de maatschappij, kunnen ze invloed hebben op publieke waarden. Om die reden is het belangrijk om nu al na te denken over de effecten van quantumtechnologie voor de maatschappij. Paragraaf 3.3 besteedt daarom aandacht aan specifieke toepassingen van quantum en de relevantie daarvan voor bepaalde publieke waarden. De publieke waarden die worden besproken zijn in kaart gebracht door middel van literatuuronderzoek. Hierbij is zowel academische literatuur geanalyseerd als zogenoemde 'grijze literatuur'.[68] Er is daarbij gekeken naar literatuur over ethische vraagstukken, verantwoorde innovatie en beleid.

65 OESO. (2024). Framework for Anticipatory Governance of Emerging Technologies. *OECD Science, Technology and Industry Policy Papers*.

66 Ibid.

67 Ibid.

68 Grijze literatuur is literatuur die niet door een uitgever is gepubliceerd, bijvoorbeeld (beleids)rapporten.

Paragraaf 3.3 bespreekt de volgende waarden: privacy, inclusie en participatie, rechtvaardigheid en menselijke integriteit, democratie en democratisering, en openheid en open strategische autonomie.[69] In de academische en grijze literatuur worden ook andere publieke waarden genoemd die buiten de reikwijdte van dit rapport vallen, zoals duurzaamheid, cybersecurity en (militaire) veiligheid. Van de hier besproken publieke waarden komen privacy, inclusie en participatie en democratie en democratisering het vaakst aan de orde in de academische literatuur. De publieke waarden rechtvaardigheid en menselijke integriteit, en openheid en open strategische autonomie komen vaker aan bod in de grijze literatuur, bijvoorbeeld in beleidsdiscussies. Zo komt de waarde openheid en open strategische autonomie naar voren in discussies over de geopolitieke dynamiek van de ontwikkeling van quantumtechnologie.

De ontwikkeling van quantumtechnologieën biedt zowel kansen als uitdagingen ten aanzien van publieke waarden. Zo kunnen quantumtechnologieën bijdragen aan de versterking van de publieke waarde veiligheid, terwijl ze de publieke waarde privacy kunnen ondermijnen. Paragraaf 3.3 bespreekt daarom per publieke waarde de kansen en uitdagingen op het niveau van quantumtechnologie in het algemeen en, waar relevant, voor de specifieke relevante toepassingsgebieden van quantum.

3.3. Kansen en uitdagingen voor publieke waarden

Inclusie en participatie

Uitdagingen

Quantumtechnologieën hebben hoge technische eisen en kosten, waardoor brede inclusiviteit en participatie niet vanzelfsprekend zijn. Naar verwachting zal een klein aantal partijen de toegang tot deze technologieën beheren, zoals grote technologiebedrijven, overheidslaboratoria of gespecialiseerde cloudplatforms. Zij zullen bepalen wie quantumcapaciteit mag gebruiken en onder welke voorwaarden.[70] Daarmee creëren quantumtechnologieën nieuwe afhankelijkheden, omdat ze inhoudelijke participatie mogelijk beperken tot een klein aantal machtige partijen.[71]

Vroege investeringen in technologie volgen vaak een vast patroon.[72] Deze investeringen komen

69 Deze waarden zijn afgestemd met een beleidsmedewerker van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

70 Lane, B., et al. (2025). *Allocating access to quantum computing: A legal-ethical framework*. QDNL.

71 United Nations Educational, Scientific and Cultural Organization. (2025). *Quantum science for inclusion and sustainability*.

72 World Economic Forum. (2024). *Quantum Economy Blueprint*.

vaak uit het Mondiale Noorden, wat kan leiden tot grotere wereldwijde ongelijkheid. Experts waarschuwen al voor een mogelijke *quantum divide*: een situatie waarin een klein aantal technologisch geavanceerde landen en bedrijven vroeg toegang krijgen tot quantumcapaciteiten, terwijl andere landen en bedrijven worden uitgesloten.[73] Uitsluiting van landen in vroege ontwikkelstadia resulteert vaak in langdurige afhankelijkheid van technologieën, standaarden en infrastructuur.[74] Als het Mondiale Zuiden niet inhoudelijk betrokken wordt, bestaat het risico dat quantumtechnologieën de bestaande digitale en geopolitieke ongelijkheden versterken, waardoor dergelijke landen passieve adoptanten in plaats van medevormgevers van deze systemen worden.

Andere uitdagingen hebben betrekking op quantumonderzoek en -onderwijs. Recente onderzoeken laten een gebrek in quantumvaardigheden zien, en bedrijven geven aan problemen te hebben om talent aan te trekken met de juiste combinatie van technische expertise en quantumkennis.[75] Op de arbeidsmarkt is er bij banen op het gebied van quantum ook sprake van een gender- en diversiteitskloof.[76] Uit recente schattingen blijkt bijvoorbeeld dat slechts 15% van de Europese quantumonderzoekers vrouw is.[77] Verder laat recent onderzoek zien dat vooral goed gefinancierde en onderzoeksgerichte instellingen toegang tot quantumcursussen en opleidingen hebben, terwijl veel studenten uit gezinnen met lage inkomens en uit niet-stedelijke gebieden niet worden bereikt.[78] Deze inzichten suggereren dat vaardigheden en besluitvorming bij slechts een beperkte groep terecht kunnen komen, wat zorgt voor belemmeringen voor bredere participatie aan de ontwikkeling van quantumtechnologieën. Deze ongelijkheden zouden bovendien kunnen worden versterkt in latere fasen van innovatie en governance.

Experts waarschuwen daarnaast dat de complexiteit van quantumtechnologieën niet-specialisten kan uitsluiten van betrokkenheid bij belangrijke besluitvormingsprocessen. Dat zou de ruimte voor participatie nog verder beperken.[79] Quantumtechnologieën zijn gebaseerd op een

---

73 Bridging the quantum divide. (2025) *Nature Reviews Electrical Engineering*.
Vermaas, P., & Mans, U. (2024). *Quantum Technologies and their Global Impact*. QDNL.
Ten Holter, C., et al. (2022). Bridging the quantum divides: A chance to repair classic(al) mistakes? *Quantum Science and Technology*.
74 Arthur, W. B. (1989). Competing technologies, increasing returns, and lock-in by historical events. *The Economic Journal*.
75 Greinert, F., et al. (2024). Advancing quantum technology workforce: industry insights into qualification and training needs. *EPJ Quantum Technology*.
76 Zie bijvoorbeeld: European Commission: Directorate-General for Research and Innovation. (2025). *She figures 2024. Gender in research and innovation – Statistics and indicators*. Publications Office of the European Union.
77 European Cooperation in Science & Technology. (2022, 18 oktober). *Women in quantum technologies*.
78 Meyer, J. C., et al. (2024) Disparities in access to U.S. quantum information education. *Physical Review Physics Education Research*.
79 Vermaas, P. E. (2017). The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable.

theorie die algemeen wordt beschouwd als contra-intuïtief en moeilijk te doorgronden, waardoor ze voornamelijk toegankelijk zijn voor een kleine groep van specialisten. Het is lastig om deel te nemen aan het publieke debat over de ontwikkeling van quantumtechnologie wanneer je geen redelijke kennisbasis hebt over quantumtheorie en de daaruit voortvloeiende (technische) gevolgen.[80] Daardoor worden belangrijke beslissingen over bijvoorbeeld financieringsprioriteiten, toepassingen en maatschappelijke gevolgen met name genomen door experts en (quantum)instellingen. Zo blijft er minder ruimte over voor een inclusief maatschappelijk debat.

Kansen

Quantumtechnologieën bieden kansen om uitsluiting te vermijden. Dat komt doordat ze zich nog in een stadium bevinden waarin inclusie en participatie vanaf het begin kunnen worden meegenomen, in plaats van pas achteraf nadat zich al vormen van uitsluiting of andere ongewenste effecten hebben voorgedaan.[81] Het bevorderen van bredere participatie en inclusie kan de kans vergroten op maatschappelijk relevante use cases. Bovendien ondersteunt dit de *maker movement*, waarbij innovatie voortkomt uit diverse achtergronden, disciplines en lokale behoeften in plaats van dat deze geconcentreerd is bij een klein aantal partijen.[82] Experts benadrukken dat open-accessdiensten voor *quantumcloudcomputing* kansen bieden voor inclusie en participatie (zie paragraaf 2.6).[83] *Quantumcloudcomputing* vermindert financiële en technische barrières. Daardoor kunnen meer diverse partijen experimenteren met en kennis opdoen over quantumtoepassingen.[84] Denk aan universiteiten en kleine organisaties. Tegelijkertijd benadrukken onderzoekers dat deze voordelen niet vanzelfsprekend zijn. Beleid moet hierop sturen, anders kan *quantumcloudcomputing* juist leiden tot grotere ongelijkheid.[85]

De verschuiving van een deel van de computationele infrastructuur van klassieke technologie naar quantumtechnologie vraagt om nieuwe kennis en expertise. Dit biedt kansen voor bredere participatie.[86] Inclusief vormgegeven onderwijs en scholing kan toegangsdrempels verlagen en

---

Ethics and Information Technology.

80 OESO. (2024). Framework for Anticipatory Governance of Emerging Technologies. *OECD Science, Technology and Industry Policy Papers*.

81 Ten Holter, C., et al. (2022). Bridging the quantum divides: A chance to repair classic(al) mistakes? *Quantum Science and Technology*.

82 Gasser, U., et al. (2024). A call for responsible quantum technology. *Nature Physics*.

83 Lane, B., et al. (2025). *Allocating access to quantum computing: A legal-ethical framework*. QDNL.

Seskir, Z. C., et al. (2023). Democratization of quantum technologies. *Quantum Science and Technology*.

United Nations Educational, Scientific and Cultural Organization. (2025). *Quantum science for inclusion and sustainability*.

84 United Nations Educational, Scientific and Cultural Organization. (2025). *Quantum science for inclusion and sustainability*.

85 Lane, B., et al. (2025). *Allocating access to quantum computing: A legal-ethical framework*. QDNL.

86 UNESCO benadrukt dat huidige ongelijkheden minder worden veroorzaakt door ongelijke toegang tot technologieën, en meer door ongelijke participatie in fundamenteel onderzoek, vaardighedenontwikkeling en het bepalen van de onderzoeksagenda, waarbij met name het Mondiale

bestaande expertise beter benutten. Ook kan dit ervoor zorgen dat een bredere groep professionals kan meedenken over hoe quantumveilige systemen worden ontwikkeld, toegepast en beheerd. Daarmee kan de opbouw van kennis en vaardigheden rond de transitie van klassieke technologie naar quantumtechnologie bijdragen aan een inclusiever quantum-ecosysteem.

Een andere kans voor inclusie en participatie ligt in de uitbreiding van inhoudelijke betrokkenheid bij internationale onderzoeksagenda's en samenwerking. UNESCO ziet quantumwetenschap als een wereldwijde inspanning en plaatst het daarom op één lijn met doelstelling 17 van de *Sustainable Development Goals*: partnerschap om de doelen te bereiken.[87] Vanuit dit perspectief worden internationale en multilaterale initiatieven gezien als belangrijke kansen om te zorgen voor meer participatie, vereenvoudiging van kennisuitwisseling en voorkomen dat expertise en macht bij een klein aantal landen komen te liggen.[88]

Privacy

Uitdagingen

De ontwikkeling van quantumtechnologieën brengt privacyrisico's mee. Quantumsensing, -computing en-comunicatie hebben elk eigen, maar ook onderling samenhangende, gevolgen voor de wijze waarop data verkregen, bewaard en bewerkt kunnen worden. Sommige experts waarschuwen voor het risico dat deze ontwikkelingen de dynamiek van een surveillancesamenleving kunnen versterken. In het dagelijks leven kan grootschalige verzameling, geautomatiseerde analyse en het strategisch inzetten van persoonsgegevens structureel ingebed raken. Dit kan ingrijpendere en minder transparante vormen van monitoring en sociale controle mogelijk maken.[89]

Zuiden wordt getroffen. Zie: United Nations Educational, Scientific and Cultural Organization. (2025). *Quantum science for inclusion and sustainability*.

87 United Nations Educational, Scientific and Cultural Organization. (2025). *Quantum science for inclusion and sustainability*.

88 Arthur, W. B. (1989). Competing technologies, increasing returns, and lock-in by historical events. *The Economic Journal*.

89 Inglesant, P., et al. (2016). *Thinking ahead to a world with quantum computers: The landscape of responsible research and innovation in quantum computing*. Networked Quantum Information Technologies.

Een risico is dat een voldoende geavanceerde quantumcomputer de bestaande cryptografiesystemen kan kraken.[90] Deze systemen vormen de basis voor bijvoorbeeld veilig internetten en digitale identificatiesystemen. Een organisatie met toegang tot zo'n quantumcomputer zou ervoor kunnen zorgen dat gevoelige informatie wordt ontsleuteld. Dat maakt het risico op een *quantum divide* nog groter. Er kan namelijk een ongelijk privacylandschap ontstaan als sommige partijen de transitie naar quantum sneller maken, waarbij gevoelige data van minder goed voorbereide landen of actoren kwetsbaar worden voor onderschepping of exploitatie. Dit risico wordt geïllustreerd door de *harvest now, decrypt later*-strategie. Hierbij worden versleutelde data nu al onderscherpt en bewaard, in de verwachting dat de vooruitgang in (quantum)computers ervoor zorgt dat de versleuteling in de toekomst gekraakt kan worden, en de data daarmee inzichtelijk worden.[91] Deze strategie kan zorgen voor een fundamentele verandering van de opvattingen over privacy. Bescherming van digitale communicatie en informatie hangt dan namelijk niet alleen meer af van continue monitoring in het heden, maar moet er ook rekening mee houden dat encryptie gekraakt kan worden in de toekomst.[92]

Andere risico's hebben te maken met algoritmen die verbeterd worden door quantum (zie paragraaf 2.3). Deze algoritmen maken een efficiëntere analyse van complexe en grote datasets mogelijk.[93] Dergelijke ontwikkelingen kunnen samen worden gezien met de opkomst van een 'algoritmische maatschappij' waarin *machinelearning*-systemen een steeds centralere rol spelen tussen enerzijds de digitale en anderzijds de fysieke en sociale wereld.[94] Vooruitgang op quantumgebied heeft de potentie om bestaande privacy-uitdagingen te vergroten, bijvoorbeeld doordat quantum geavanceerdere patroonherkenning mogelijk maakt. Hierdoor neemt het risico op indirecte surveillance toe, zoals profilering en voorspelling van gedrag, op steeds ondoorzichtigere manieren. Dit maakt vraagstukken rond privacy en gegevensbescherming nog complexer.

Ook quantumsensoren kunnen leiden tot privacy-uitdagingen. Ze kunnen namelijk heel nauwkeurig informatie vastleggen over locaties, bewegingen of tijdstippen.[95] Zo kunnen

90 Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134).

91 Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*.

92 Olsson, E., & Öhman, C. (2025). The quantum panopticon: A theory of surveillance for the quantum era. *Minds and Machines*.

93 Biamonte, J., et al. (2017). Quantum machine learning. *Nature*.

94 European Cooperation in Science & Technology. (2022, 18 oktober). *Women in quantum technologies*.

95 Degen, C. L., et al. (2017). Quantum sensing. *Reviews of Modern Physics*.

Taddeo, M., et al. (2024). Consider the ethical impacts of quantum technologies in defence—before it's too late. *Nature*.

navigatie of gravimetrische sensoren[96] die met quantum zijn verbeterd bewegingen van individuen afleiden zonder gebruik te maken van externe referentiesignalen zoals gps.[97] Daardoor kunnen mensen gemonitord worden zonder dat ze zich daarvan bewust zijn. Dat roept zorgen op over geïnformeerde toestemming en proportionaliteit.[98]

Kansen

Quantumtechnologieën kunnen om meerdere redenen zorgen voor verbeterde privacy. Ten eerste kan quantumversleuteling de privacy mogelijk sterker waarborgen dan klassieke versleuteling. Quantumversleuteling is gebaseerd op de fysieke eigenschappen van quantumsystemen, zodat niet-detecteerbare onderschepping onmogelijk wordt.[99] Daardoor blijft gevoelige communicatie vertrouwelijk, zelfs voor kwaadwillende partijen met krachtige quantumcomputers. Dit ondervangt ook langetermijnrisico's, zoals de eerder besproken *harvest now, decrypt later*-strategie.[100]

Ten tweede biedt het quantuminternet een kans om de privacy te verbeteren op het niveau van de communicatie-infrastructuur. Quantumnetwerken kunnen de verzending van in quantumtoestanden gecodeerde informatie mogelijk maken. Dat zorgt voor veiligere communicatie die bestand is tegen onderschepping.[101] Ten derde kunnen opkomende protocollen het mogelijk maken dat gebruikers op afstand computerberekeningen kunnen doen op quantumsystemen, zonder hun gegevens bekend te maken.[102] In de toekomst is dus voor toegang tot digitale diensten mogelijk niet automatisch het delen van (persoonlijke of vertrouwelijke) gegevens nodig.

In bredere zin biedt vooruitgang op quantumgebied ook een kans om opnieuw na te denken over privacy als een eigenschap van digitale infrastructuren. Wanneer privacywaarborgen direct worden ingebed in de technische architectuur, kunnen quantumsystemen *privacy-by-design* beter verankeren. Privacy hangt dan namelijk minder af van de vraag hoe organisaties dit hebben

96 Bongs, K., et al. (2023). Quantum sensors will start a revolution – if we deploy them right. *Nature*.

97 Kitching, J., et al. (2011). Atomic sensors – A review. *IEEE Sensors Journal*.

98 Taddeo, M., et al. (2024). Consider the ethical impacts of quantum technologies in defence—before it's too late. *Nature*.

99 Biamonte, J., et al. (2017). Quantum machine learning. *Nature*.

100 Vermaas, P. E. (2017). The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable. *Ethics and Information Technology*.

101 Vermaas, P., et al. (2019). *Quantum internet: The internet's next big step*. TU Delft.

102 Broadbent, A., et al. (2009). Universal blind quantum computation. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (pp. 517–526). IEEE.

geregeld of hoe goed gebruikers opletten. Dit kan er bovendien toe leiden dat er meer aandacht komt voor het genereren, verwerken en delen van informatie.

Rechtvaardigheid en menselijke integriteit

Uitdagingen

Quantumtechnologieën brengen uitdagingen mee op het gebied van rechtvaardigheid en menselijke integriteit. Dat komt vooral doordat ze kunnen zorgen voor sociaaleconomische voordelen voor bepaalde groepen en een ongelijke verdeling van macht. Naarmate quantumtechnologie steeds nauwer verweven raakt met strategische concurrentie of economische veiligheid, dreigen innovatietrajecten te bepalen wie profiteert van technologische vooruitgang en wie de risico's draagt.

Wereldwijd roept de al besproken *quantum divide* zorgen op over potentiële ongelijkheden als gevolg van quantumtechnologieën. De ontwikkeling van quantum is namelijk sterk geconcentreerd in minder dan vijftien landen,[103] die daarmee ook de infrastructurele en agendabepalende macht zijn. Tegelijkertijd lopen grote delen van de wereld het risico op langdurige afhankelijkheid en verminderde beleidsautonomie, met name het Mondiale Zuiden. Rechtvaardigheidsvraagstukken worden verder versterkt wanneer landen quantumtechnologieën beschouwen als strategische middelen in een nul-som-logica.[104] Dan komen de voordelen van quantumtechnologieën vooral ten goede aan vroege instappers, terwijl de rest te maken krijgt met de kwetsbaarheden, zoals blootstelling aan spionage, toezicht, exploitatie of economische dwang. Dit kan leiden tot een structureel onrechtvaardige verdeling van de baten en lasten.

Een andere zorg is mogelijk misbruik van quantumcomputing.[105] Zo zouden sommige overheden quantumcomputing en geavanceerdere, minder goed detecteerbare vormen van staatstoezicht kunnen gebruiken om hun autoritaire macht te versterken.

De integratie van quantumcapaciteit in *machinelearning*-systemen[106] kan ervoor zorgen dat ook sectoren als de gezondheidszorg of rechtshandhaving hier gebruik van gaan maken. Dat kan ingrijpende gevolgen hebben. Personen kunnen gediscrimineerd of nadelig behandeld worden,

103 United Nations Educational, Scientific and Cultural Organization. (2025). *Quantum science for inclusion and sustainability*.
104 Ibid.
105 Taddeo, M., et al. (2024). Consider the ethical impacts of quantum technologies in defence—before it's too late. *Nature*.
106 European Cooperation in Science & Technology. (2022, 18 oktober). *Women in quantum technologies*.

doordat de verbeterde rekenkracht verbanden kan leggen die eerder niet mogelijk waren.[107] Het World Economic Forum noemt bijvoorbeeld dat quantumtechnologieën onrechtvaardigheden kunnen versterken.[108] Kapitaalkrachtigere actoren profiteren daarvan, terwijl minder bedeelde groepen structurele belemmeringen kunnen ondervinden.

Kansen

Quantumtechnologieën kunnen bijdragen aan rechtvaardigere en verantwoorde systemen als ze worden toegepast als hulpmiddel, en niet om menselijke beoordeling te vervangen. Quantumtechnologieën moeten ingebed zijn in robuuste ethische en institutionele kaders, zoals de AI-verordening doet op het gebied van kunstmatige intelligentie. Zoals eerder genoemd, liggen er voornamelijk kansen in vroege stadia waarin toepassingen nog verder uitgewerkt moeten worden. Dan is er namelijk nog invloed uit te oefenen op de manier waarop quantumtechnologieën worden ontworpen en gebruikt in de praktijk.

Zo zijn er mogelijkheden voor internationale samenwerking.[109] De concentratie van quantumcapaciteit kan leiden tot afhankelijkheden tussen het Mondiale Noorden en het Mondiale Zuiden. Dit benadrukt het belang van internationationale kaders waarin gedeelde standaarden en inclusieve participatie gezamenlijk worden vormgegeven. Er liggen kansen voor rechtvaardigheid door het vormgeven van normen over interoperabiliteit, post-quantum-cryptografie, onderwijs en de verantwoorde toepassing van quantumtechnologie. Dat moet worden gedaan op een manier die afhankelijkheden van specifieke technologieën of leveranciers beperkt en waarbij de autonomie van minder kapitaalkrachtige of minder goed toegeruste landen en organisaties behouden blijft.

Quantumtoepassingen kunnen daarnaast kansen bieden om capaciteitsproblemen op te lossen, zoals in de rechtspraak. De tijdige toegang tot de rechter wordt op dit moment ondermijnd door de grote hoeveelheid te behandelen zaken en een overvloed aan informatie. Vooral personen die over minder middelen beschikken ondervinden hier nadeel van. Quantumtoepassingen voor informatieverwerking of -optimalisering kunnen helpen bij de verwerking van grote hoeveelheden informatie en een effectievere inzet van middelen.[110] Een voorbeeld is het algoritme van Grover. Dit kan zoekopdrachten binnen grote, ongesorteerde databases

107 OESO. (2025). A quantum technologies policy primer. *OECD Digital Economy Papers*.
108 Effoduh, J. O. (2025, 7 mei). Quantum justice: How could quantum computing transform the legal system? *World Economic Forum*.
109 Gasser, U., et al. (2024). A call for responsible quantum technology. *Nature Physics*.
110 Bongs, K., et al. (2023). Quantum sensors will start a revolution – if we deploy them right. *Nature*.

versnellen. Dit moet vooral worden gezien als een kans om professionals te ondersteunen bij de afhandeling van complexe zaken, en niet om beoordelingen volledig te automatiseren.

Democratie en democratisering

Uitdagingen

De uitdagingen die quantumtechnologieën vormen voor democratie en democratisering vloeien vooral voort uit het feit dat deze technologieën verstrekkende maatschappelijke gevolgen kunnen hebben, terwijl het lastig is voor veel mensen om, door een gebrek aan expertise, deel te nemen aan het publieke debat hierover en demodratische controle uit te oefenen. Dit wordt verder versterkt doordat quantumtechnologieën kunnen samenvloeien met strategische overwegingen, zoals over veiligheid. Dit kan ertoe leiden dat belangrijke beslissingen over onderzoeksprioriteiten of toepassingen zich verplaatsen naar ondoorzichtige, door experts gedomineerde domeinen, waar democratisch toezicht beperkt is. Daardoor ontstaat ook het risico dat het vertrouwen van het publiek in instituties wordt aangetast, waardoor het vertrouwen in democratische processen wordt ondermijnd en de maatschappelijke voordelen die deze technologieën beogen te leveren, worden beperkt.[111]

Doordat quantumtechnologie vraagt om specifieke expertise en kapitaalintensieve infrastructuren, leidt dit al snel tot een concentratie van de besluitvormingsmacht, bijvoorbeeld bij ingenieurs, wetenschappers, veiligheidsorganisaties of bedrijven. Deze concentratie staat haaks op de democratische idealen voor bredere participatie en verantwoordelijkheid.[112] De vroege toegang van grote technologiebedrijven tot belangrijke quantumontwikkelingen kan zich bijvoorbeeld vertalen in onevenredige politieke invloed. Dat is vooral het geval wanneer quantumcapaciteiten worden geleverd aan overheden in ruil voor invloed, bijvoorbeeld op regelgeving. Dit maakt deze bedrijven minder vatbaar voor overheids- of maatschappelijk toezicht.[113]

Een andere uitdaging is de vormgeving van publiek debat. Bij strategische keuzes zijn vaak vooral directe stakeholders, zoals overheden, het bedrijfsleven en experts betrokken. Indirect betrokkenen, zoals het maatschappelijk middenveld, worden eerder beschouwd als passieve informatieontvangers in plaats van als deelnemers. Onderzoekers waarschuwen dat deze benadering mogelijk leidt tot uitsluiting, waarbij kleine groepen achter gesloten deuren

111 Van Der Weij, F., et al. (2023). Value change and technological design. *IEEE Technology and Society Magazine*.
112 Seskir, Z. C., et al. (2023). Democratization of quantum technologies. *Quantum Science and Technology*.
113 Vermaas, P., et al. (2019). *Quantum internet: The internet's next big step*. TU Delft.

overleggen, in plaats van dat er brede participatie plaatsvindt.[114] Wanneer het publiek pas betrokken wordt nadat besluiten al zijn genomen, is de democratische input beperkt tot raadpleging zonder inhoudelijke macht. Het risico is dat daarmee de democratische rechtstaat in kracht afneemt, doordat sommige actoren alleen worden uitgenodigd te reageren op vooraf bepaalde trajecten, in plaats van dat zij de doelen en grenzen van quantuminnovatie mede vorm kunnen geven.[115]

Experts waarschuwen verder dat quantumtechnologieën niet alleen moeten worden bekeken vanuit het perspectief van nationale veiligheid. Vanuit veiligheidsoverwegingen worden geheimhouding en besloten besluitvormingsprocessen soms gelegitimeerd, vaak onder het mom van de noodzaak van de bescherming van strategische belangen.[116] In bepaalde sitauties is dat verdedigbaar, maar bredere, onrechtmatige toepassing ervan brengt het risico met zich mee dat dergelijke processen, die transparantie en democratisch toezicht opzij schuiven, worden genormaliseerd. Dit beperkt burgers om de technologische toekomst mede vorm te geven: hun belangen worden aangenomen, in plaats van duidelijk uitgesproken.[117]

Tot slot brengen quantumveilige communicatiekanalen uitdagingen met zich mee. Door hun ontwerp kunnen deze kanalen de transparantie en zichtbaarheid van (overheids)communicatie verminderen. Hierdoor kan het risico op wangedrag door partijen met exclusieve toegang afnemen, terwijl de verleiding ertoe juist kan toenemen.[118] Besluitvormingsprocessen die normaal gesproken onderwerp zijn van parlementaire, journalistieke of maatschappelijke controle kunnen technisch ondoorzichtig worden. Dat zou de ruimte verminderen voor democratische verantwoording.

Kansen

Er liggen vooral kansen om de ontwikkeling van quantumtechnologie in overeenstemming te brengen met democratische waarden in het vormgeven van de voorwaarden waaronder deze technologieën worden ontwikkeld, zoals op het gebied van transparantie en democratische

114 Seskir, Z. C., et al. (2023). Democratization of quantum technologies. *Quantum Science and Technology*.

115 Vermaas, P., et al. (2019). *Quantum internet: The internet's next big step*. TU Delft.

116 Vermaas, P. E. (2017). The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable. *Ethics and Information Technology*.

117 Ibid.

118 El-Sheimy, N., & Youssef, A. (2020). Inertial sensors technologies for navigation applications: State of the art and future trends. *Satellite Navigation*.

controle.[119] Zo kunnen een sterkere betrokkenheid van belanghebbenden, en regels voor toegang tot gedeelde quantuminfrastructuren tegenwicht bieden aan de eerder besproken tendens richting machtsconcentratie.[120] Daarom betekent democratisering in deze context niet zozeer universele deelname bij technische beslissingen, maar gaat het om de institutionalisering van inclusievere manieren waarlangs de maatschappij invloed kan uitoefenen op strategische beslissingen.[121]

Een andere kans is dat quantumtoepassingen democratieversterkende processen direct kunnen ondersteunen. Quantumcommunicatie en stemprotocollen zouden in de toekomst bijvoorbeeld garanties kunnen bieden voor geheimhouding en anonimiteit bij het stemmen op een manier die met klassieke systemen niet mogelijk is. Zo laten recente experimenten zien dat quantum-stemsystemen het stemgeheim kunnen beschermen, terwijl ze tegelijkertijd verifieerbaar blijven en bestand zijn tegen externe inmenging en manipulatie.[122] Voor bijvoorbeeld de registratie van kiezers of het verzenden van stembiljetten kan dit de risico's wegnemen van vervalsing of ontsleuteling. Dat kan het vertrouwen versterken in technische infrastructuren die de basis vormen van democratische besluitvorming.

Openheid en open strategische autonomie

Uitdagingen

Open strategische autonomie heeft gevolgen voor het delen van kennis. Het streven naar soevereiniteit in de ontwikkeling van quantum heeft wereldwijd tot minder overheidsfinanciering voor internationale samenwerking geleid en tot toegenomen concurrentie tussen landen om een leidende positie in quantumtechnologie.[123]

Een van de uitdagingen is het effect van beperkte openheid op onderzoek en internationale samenwerking. Onderzoekers en onderzoeksinstellingen moeten tegenwoordig steeds meer aandacht besteden aan de vraag met wie zij kunnen samenwerken. Dit wordt steeds meer bepaald vanuit economische en veiligheidsoverwegingen, in plaats van door

119 Vermaas, P. E. (2017). The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable. *Ethics and Information Technology*.
Barreneche, A., et al. (2026, 12 januari). Quantum technologies and the role of governments and policy in kickstarting the second revolution. *OECD*.
120 Vermaas, P. E. (2017). The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable. *Ethics and Information Technology*.
121 Ibid.
122 Laurent-Puig, N., et al. (2025). Experimental quantum electronic voting. *arXiv*.
123 Briegel, H. J., et al. (1998). Quantum repeaters: The role of imperfect local operations in quantum communication. *Physical Review Letters*.

onderzoeksprioriteiten en kwaliteit. Open strategische autonomie kan daarom ook steeds meer worden gekoppeld aan kennisveiligheid.[124] Dit heeft concrete gevolgen. Zo zijn er zorgen dat verminderde internationale samenwerking kan leiden tot een situatie met meerdere suboptimale platforms voor quantumcomputing in de EU, in plaats van de gewenste, en efficiëntere, situatie met enkele excellente platforms.[125]

Geopolitieke concurrentie en veiligheidszorgen bij onderzoekssamenwerking kunnen ook leiden tot gesloten nationale ecosystemen, zonder samenwerking met internationale partners.[126] Zo kunnen er meer voorwaarden worden verbonden aan internationale wetenschappelijke samenwerkingen, wat de kennisuitwisseling kan beperken.[127] Zogenoemd 'moreel isolationisme' kent daarmee één concrete uitdaging voor technologisch protectionisme: dergelijk protectionisme en een gebrek aan internationale samenwerking kunnen het potentieel van quantumtechnologieën beperken om wereldwijde maatschappelijke uitdagingen aan te pakken.[128] Ook dat kan opkomende economieën uitsluiten van de voordelen van quantumtechnologieën.

Kansen

Open strategische autonomie kan kansen bieden voor landen als Nederland om voor meer technologische ontwikkeling te zorgen in het algemeen en nationaal belang. Overheidsfinanciering kan de ontwikkeling en het gebruik van quantumtechnologieën ondersteunen, in lijn met nationale prioriteiten en maatschappelijke uitdagingen.[129] De Nationale Agenda Quantumtechnologie uit 2019 stelt dat quantum van strategisch belang is, zowel voor het aanpakken van maatschappelijke uitdagingen als voor de autonomie van Nederland. Er wordt daarom benadrukt dat het belangrijk is om de agenda te implementeren en tegelijk de soevereiniteit te beschermen.[130]

124 Adviesraad voor wetenschap, technologie en innovatie. (2022). *Kennis in conflict. Veiligheid en vrijheid in balans*.
125 Liman, A., & Weber, K. (2023). Quantum computing: Bridging the national security–digital sovereignty divide. *European Journal of Risk Regulation*.
126 Biamonte, J., et al. (2017). Quantum machine learning. *Nature*.
127 Briegel, H. J., et al. (1998). Quantum repeaters: The role of imperfect local operations in quantum communication. *Physical Review Letters*.
128 Shelley-Egan, C., & Vermaas, P. (2024). European technological protectionism and the risk of moral isolationism: The case of quantum technology development. *Journal of Responsible Technology*.
129 OESO. (2025). A quantum technologies policy primer. *OECD Digital Economy Papers*.
130 QDNL. (2019). *Nationale Agenda Quantumtechnologie*.

Hoewel soevereiniteit zonder meer belangrijk is, kan het combineren van grensoverschrijdende financieringsinitiatieven dubbel werk voorkomen en de impact van publieke en private investeringen in quantumtechnologieën vergroten.[131] Door samen te werken kunnen landen schaalvoordelen realiseren en sterkere prikkels creëren voor investeringen in onderzoek en innovatie. Hierdoor kunnen grootschalige projecten haalbaarder en kostenefficiënter worden.

131 Briegel, H. J., et al. (1998). Quantum repeaters: The role of imperfect local operations in quantum communication. *Physical Review Letters*.

4. Quantumtechnologieën, recht en fundamentele rechten

Dit hoofdstuk brengt vanuit juridisch perspectief de gevolgen van quantumtechnologieën voor het beschermen en uitoefenen van fundamentele rechten in kaart. Hierbij wordt gekeken naar relevante wet- en regelgevingsinstrumenten. Deze wetten en regels behoren tot de belangrijkste manieren om publieke waarden bij nieuwe technologieën te beschermen. Fundamentele rechten spelen een essentiële rol om de bescherming van publieke waarden te waarborgen wanneer individuele rechten en collectieve belangen op het spel staan.

Over het algemeen bevinden quantumtechnologieën zich nog niet in een ontwikkelingsfase waarin de toepassing ervan specifieke nieuwe juridische implicaties of gevolgen voor fundamentele rechten met zich meebrengt. Dit hoofdstuk brengt daarom in kaart hoe quantumtechnologieën juridisch kunnen worden gekarakteriseerd, en identificeert de belangrijkste juridische instrumenten en fundamentele rechten die mogelijk door quantuminnovaties worden geraakt. De analyse kijkt daarbij door de bril van digitale infrastructuren naar de juridische gevolgen van quantumtechnologieën. Quantumcomputing, -communicatie en -sensing zullen namelijk, als ze op grote schaal toepasbaar zijn, bepaalde verbeteringen met zich meebrengen voor de kernfuncties van onze digitale infrastructuur.

Paragraaf 4.1 geeft een algemeen overzicht van de wet- en regelgevingsinstrumenten voor fundamentele rechten die relevant zijn voor quantumtechnologieën. Paragraaf 4.2 en 4.3 gaan in op de potentiële implicaties voor fundamentele rechten door quantumcomputing, zoals op het gebied van communicatie- en informatieveiligheid. Paragraaf 4.4 gaat in op quantumsensing en de juridische vragen die daar relevant zijn, waaronder voor privacy en gegevensbescherming. Tot slot bespreekt paragraaf 4.5 een aantal structurele overwegingen over quantumtechnologieën en fundamentele rechten, waaronder digitale soevereiniteit.

4.1. Wet- en regelgevingsinstrumenten

De afgelopen decennia voerde de Europese Unie een uitgebreid stelsel van wet- en regelgeving in om fundamentele rechten in het digitale tijdperk te beschermen. Europese wetten en regels worden aangevuld met implementatie op nationaal niveau en nationaal recht.
Wet- en regelgeving is veelal technologieneutraal opgezet. Dit betekent dat de teksten van wetten en de geboden beschermingen niet afhankelijk zijn van een specifieke technologie. Zo hangt bijvoorbeeld gegevensbescherming of de bescherming van telecommunicatie niet af van bepaalde technologieën die worden gebruikt om communicatie mogelijk te maken of persoonsgegevens te verwerken. Technologieneutraliteit zorgt ervoor dat bestaande wet- en regelgeving bestand is tegen de meeste gevallen van technologische verandering zonder dat er nieuwe wetgeving nodig is.[132]

Tot de belangrijkste algemenere wetten behoren:

- het Europees Verdrag voor de Rechten van de Mens (EVRM), het Handvest van de grondrechten van de Europese Unie (Handvest), en de Nederlandse Grondwet voor de bescherming van fundamentele rechten. Mensenrechtenverdragen van de Verenigde Naties kunnen ook relevant zijn voor de interpretatie van mensenrechten in het digitale tijdperk;
- het EU-wetboek voor elektronische communicatie, de ePrivacyrichtlijn, de Digitaledienstenverordening, de Digitalemarktenverordening, en de AI-verordening voor elektronische communicatie en digitale diensten;
- het Europese en Nederlandse mededingingsrecht;
- de Algemene verordening gegevensbescherming (AVG), de Politierichtlijn, de Verordening inzake gegevensbeheer en de Dataverordening) voor gegevensbescherming;
- de *Network and Information Security Directive* (NIS2-richtlijn) en de *Digital Operational Resilience Act* (DORA) voor cyberbeveiliging.

Voor veel sectoren, zoals de gezondheidszorg en financiële sector, gelden er ook sectorspecifieke regels voor het waarborgen van de bescherming van consumenten.

4.2. Quantumcomputing: communicatie- en informatieveiligheid

Quantumtechnologieën zullen de duidelijkste gevolgen hebben voor fundamentele rechten op het gebied van veilige communicatie en informatieveiligheid. Quantumcomputers bedreigen

132 Voor een bespreking van technologieneutraliteit, zie bijvoorbeeld: Koops, B-J. (2006). Should ICT regulation be technology-neutral? In B-J Koops et al. (Reds.), *Starting points for ICT regulation. Deconstructing prevalent policy one-liners, IT & Law series* (9, pp. 77–108). T.M.C. Asser Press.

namelijk de informatieveiligheid, en als gevolg daarvan de bescherming en het uitoefenen van fundamentele rechten op het gebied van veilige communicatie en informatieveiligheid.

Een van de belangrijkste algoritmen die op een quantumcomputer zou kunnen draaien, is het algoritme van Shor. Dit algoritme, zo werd al besproken in paragraaf 2.3, kan hele grote getallen ontbinden in priemfactoren. Dit kunnen traditionele computers niet, en daarop zijn huidige versleutelingstechnieken gebaseerd. Als er een voldoende krachtige quantumcomputer is gebouwd waarop het algoritme van Shor kan draaien, zou die versleuteling niet meer veilig zijn. Zelfs als dit volgens zeer optimistische scenario's nog langer dan tien jaar duurt, zijn er nu al maatregelen nodig om deze bedreiging het hoofd te bieden. Het duurt namelijk lang om versleutelingstechnieken te ontwerpen die bestand zijn tegen quantumaanvallen. Bovendien zal de toepassing ervan in de huidige digitale infrastructuur een lang proces zijn. Daarnaast kunnen machtige partijen en landen nu al versleutelde data verzamelen om die te ontsleutelen zodra ze toegang krijgen tot een quantumcomputer (*harvest now, decrypt later* (zie ook paragraaf 3.3)). Dit benadrukt de noodzaak om waarborgen van informatieveiligheid voor de langere termijn te hebben.

Op het gebied van fundamentele rechten zijn er twee complentaire juridische perspectieven relevant voor informatieveiligheid.[133] Ten eerste hangen bepaalde fundamentele rechten direct samen met de bescherming van informatieveiligheid en zijn ze er gedeeltelijk afhankelijk van. Dat geldt voor het recht op privéleven, met inbegrip van vertrouwelijkheid van privécommunicatie, het recht op gegevensbescherming en het recht op communicatievrijheid, dat wordt beschermd door het recht op vertrouwelijkheid van communicatie en het recht op vrijheid van meningsuiting. Ten tweede vereist het uitoefenen van fundamentele rechten in het digitale tijdperk dat mensen gebruik kunnen maken van betrouwbare digitale infrastructuren. Dit is van belang voor de bescherming van alle fundamentele rechten, waaronder sociale en culturele rechten zoals gezondheid en onderwijs. Kortom, informatie- en communicatieveiligheid zijn van wezenlijk belang voor het tot stand brengen van betrouwbare digitale infrastructuren die de basis vormen voor het uitoefenen van fundamentele rechten in allerlei sociale omstandigheden en situaties.

Op wetgevend niveau zijn informatieveiligheid en de daarbij relevante fundamentele rechten beschermd door verschillende instrumenten, waaronder wetgeving voor

133 Briegel, H. J., et al. (1998). Quantum repeaters: The role of imperfect local operations in quantum communication. *Physical Review Letters*.

persoonsgegevensbescherming (AVG) en cyberbeveiliging (NIS2 en DORA). Deze wetgeving verplicht gereguleerde partijen de allernieuwste bescherming van informatieveiligheid toe te passen. Ook in de richtlijnen van toezichthouders op het gebied van informatieveiligheid wordt hier al naar verwezen.[134] Twee technieken die mogelijk kunnen bijdragen aan communicatie- en informatieveiligheid en daarmee aan het beschermen van fundamentele rechten zijn: post-quantum-cryptografie en *quantum key distribution*.

Post-quantum-cryptografie

De wetenschap werkt al meer dan twee decennia aan versleutelingssystemen die bestand zijn tegen quantumaanvallen. De ontdekking van het algoritme van Shor leidde tot het wetenschapsgebied post-quantum-cryptografie (PQC), een type versleuteling dat volgens experts niet gekraakt kan worden door quantumalgoritmen. Het Amerikaanse *National Institute of Standards* (NIST) leidt het proces om geschikte versleutelingssystemen te identificeren en te standaardiseren. In Europa hebben autoriteiten op het gebied van informatieveiligheid deze ontwikkelingen actief gevolgd en beleid vastgesteld voor een overstap naar quantumveilige versleutelingssystemen. De afgelopen jaren is gestart met de invoering van deze systemen.

De inspanningen van het NIST om tot nieuwe versleutelingssystemen te komen, zijn redelijk succesvol. Toch is de vraag hoe veilig de nieuwe systemen echt zijn. Zo lijkt het onmogelijk harde garanties te geven dat ze bestand zijn tegen een aanval. Experts geloven dat de nieuwe versleutelingssystemen aanvallen onmogelijk maken. Maar de systemen zijn complex en het is daarom mogelijk dat er in de toekomst toch aanvallen ontdekt worden. Hoe dan ook blijft het essentieel dat experts de best mogelijke algoritmen en toepassingen blijven zoeken om de bescherming van fundamentele rechten te waarborgen.

Een belangrijk breder beginsel voor het inrichten van onze cryptografische systemen is *crypto-agility*. Hiermee wordt de mogelijkheid bedoeld om gemakkelijker wijzigingen aan te brengen in versleutelingssystemen voor digitale infrastructuren. *Crypto-agility* is een belangrijk groter doel van post-quantum-cryptografiebeleid, een doel dat nog steeds waardevol is ook als quantumcomputers nooit de omvang bereiken die nodig is om onze huidige versleutelingssystemen te kraken. *Crypto-agility* kan namelijk zorgen voor het sneller en effectiever toepassen van de best mogelijke maatregelen voor informatieveiligheid.

---

134 Voor een bespreking van technologieneutraliteit, zie bijvoorbeeld: Koops, B-J. (2006). Should ICT regulation be technology-neutral? In B-J Koops et al. (Reds.), *Starting points for ICT regulation. Deconstructing prevalent policy one-liners, IT & Law series* (9, pp. 77–108). T.M.C. Asser Press.

Quantum key distribution

Sommige experts wijzen op quantumcommunicatietechnologieën en *quantum key distribution* (QKD) om digitale communicatie quantumveilig te maken. QKD is de belangrijkste toepassing van quantumcommunicatie. Zoals besproken in paragraaf 2.4, maakt QKD het mogelijk om versleutelingscodes op een veilige manier uit te wisselen. Dit kan invloed hebben op de bescherming van het recht op privécommunicatie. Breed gebruik van QKD zou de gelijke toegang tot veilige communicatie kunnen inperken, omdat quantumcommunicatie aanzienlijke uitgaven voor speciale hardware vereist en daarmee niet voor iedereen toegankelijk zou zijn.

Naar verwachting gaan quantumcommunicatietechnologieën de elektronische communicatienetwerken en bestaande versleutelingssystemen niet vervangen. QKD kan ook niet worden gezien als een alternatief voor post-quantum-cryptografie. Het heeft enkele mogelijke toepassingen die het nuttig maken voor bescherming tegen onrechtmatige onderschepping van communicatie, maar het zou steeds bestaan naast algemenere digitale quantumveilige versleutelingssystemen. Wel is het mogeljk nodig om op termijn wettelijke kaders te ontwikkelen voor quantumcommunicatie en QKD, met name om normen voor informatieveiligheid, interoperabiliteit en rechtmatige toegang tot communicatie te waarborgen.

4.3. Quantumcomputing: fundamentele wetenschap, optimalisatie en machinelearning

Quantumcomputing zal, naast het algoritme van Shor, mogelijk ook veel invloed hebben door de toepassing ervan in de fundamentele wetenschap, en in mindere mate op het gebied van optimalisatie en *machinelearning*. In deze paragraaf wordt aan de hand van deze domeinen ingegaan op de verdere mogelijke gevolgen van quantumcomputing voor fundamentele rechten. Belangrijk daarbij is dat deze gevolgen pas werkelijkheid worden als er een quantumcomputer van aanzienlijk formaat is gebouwd. Dat ligt op dit moment nog niet binnen handbereik.

Fundamentele wetenschap

Op het gebied van materiaalwetenschap en (bio)chemie zijn de juridische relevante gevolgen vooralsnog vooral indirect. Wanneer quantumcomputers bijdragen aan doorbraken in deze domeinen, kunnen ze leiden tot de ontwikkeling van innovaties in allerlei andere sectoren. Het is echter te vroeg om te speculeren over de eventuele juridische gevolgen hiervan. Er zijn geen aanwijzingen dat quantumtechnologie op de korte tot middellange termijn de regelgeving op dit gebied ingrijpend zal veranderen. De belangrijkste juridische uitdaging is waarschijnlijk het

functioneren van intellectuele-eigendomsstelsels en dat er misbruik kan ontstaan als de quantumcomputingmarkt wordt gedomineerd door één of een klein aantal bedrijven. Dit kan worden ondervangen door marktontwikkelingen en marktconcentratie in de quantumsector te monitoren, net als de gevolgen van dergelijke concentraties voor andere markten en sectoren.

Optimalisatie en machinelearning

Quantumcomputing gaat naar verwachting mogelijkheden bieden om berekeningen op het gebied van optimalisering en *machinelearning* te versnellen. Dit zijn belangrijke toepassingsgebieden binnen de moderne informatietechnologie en ze vormen een belangrijke basis voor de digitalisering en algoritmisering van de samenleving. Ontwikkelingen op deze terreinen hebben aanzienlijke gevolgen voor fundamentele rechten, zoals vrijheid van communicatie, privacy, gegevensbescherming en non-discriminatie. Daarom kunnen toepassingen van quantumcomputing die de prestaties van optimalisatie- en *machinelearning*-methoden verbeteren een aanzienlijke maatschappelijke impact hebben.

Het is momenteel echter nog niet duidelijk hoe groot deze gevolgen in de praktijk zullen zijn. Een van de belangrijkste quantumalgoritmen op dit gebied, het algoritme van Grover (zie paragraaf 2.3), biedt alleen kwadratische versnelling. Over het algemeen zijn de verbeteringen die quantumalgoritmen in deze toepassingsgebieden opleveren beperkter dan bij het algoritme van Shor of de voordelen van quantumsimulaties voor het begrijpen van fysische quantumsystemen. Daarnaast blijft de rekenkracht van quantumcomputers waarschijnlijk nog heel lang veel kleiner dan die van klassieke computers. Dat maakt beloofde versnellingen meestal meer theoretisch dan praktisch interessant, ook op de lange termijn. Een ander actief onderzoeksgebied is *quantum inspired computing*. Dit gaat om het gebruik van technieken uit de wiskunde en computerwetenschap die worden ingezet voor quantum-informatieverwerking bij het ontwerpen van nieuwe algoritmen die draaien op klassieke computers. Dit kan leiden tot nieuwe doorbraken in de computerwetenschap, maar dit is niet hetzelfde als een toepassing van quantumcomputers zelf.

Quantumcomputing heeft daarmee naar verwachting vooralsnog geen directe gevolgen voor bestaande regelgeving op het gebied van optimalisatie en *machinelearning*. Toch bestaan er belangrijke vragen over hoe het gebruik van algoritmen voor optimalisatie en geautomatiseerde besluitvorming het best gereguleerd kan worden om fundamentele rechten te beschermen. Deze vragen zijn blijvend relevant, ongeacht de waarschijnlijk bescheiden invloed van quantumtechnologieën op deze gebieden de komende tien tot twintig jaar.

De beste aanpak vanuit het perspectief van *anticipatory governance* is tweeledig. Ten eerste is het aan te raden om dit te benaderen vanuit het brede vraagstuk van de regulering van (klassieke) algoritmen, en ten tweede is het van belang de ontwikkelingen op het gebied van quantumalgoritmen te volgen om te zien welke nieuwe juridische en maatschappelijke vraagstukken er ontstaan.[135] Voorbeelden van problemen met algoritmen in het algemeen (en niet specifiek voor quantumtechnologie) hebben betrekking op eerlijkheid en de mogelijk discriminerende gevolgen van algoritmische besluitvorming, of transparantie en rechtsbescherming, privacy en gegevensbescherming, en de vrijheid van meningsuiting.

Toegang tot quantumcomputing

Een ander belangrijk vraagstuk in het kader van optimalisatie en *machinelearning* is de toegang tot quantumcomputing (en andere vormen van geavanceerde rekenkracht). Aan de ene kant zullen actoren de toegang tot quantumcomputers willen waarborgen voor wetenschap en innovatie, net als gebeurde met supercomputing.[136] Aan de andere kant kunnen quantumcomputers misbruikt worden en schade toebrengen aan de maatschappij. Wet- en regelgeving zal een belangrijke rol spelen om dit te voorkomen of effectief aan te pakken. Naar verwachting zullen de wettelijke kaders voor toegang tot quantumcomputing zich verder ontwikkelen naarmate de technologie volwassener wordt. Europese regelgeving voor *high-performance computing* (HPC) bevat al instrumenten voor toegang tot quantumcomputing als een nieuwe vorm van supercomputing.[137]

Tegelijkertijd ontstaan er ook beperkingen op de toegang tot quantumcomputing. Bijvoorbeeld in de vorm van exportcontrole en kennisveiligheidseisen. Dergelijke maatregelen kunnen gevolgen hebben voor het uitoefenen van de fundamentele rechten van partijen die werken aan quantuminnovatie. Zo kunnen strengere kennisveiligheidseisen gevolgen hebben voor het recht op wetenschap en onderwijs van studenten en wetenschappers. Bijvoorbeeld doordat het mogelijk vormen van uitsluiting en discriminatie in de hand kan werken.[138] Dit zijn relevante kwesties voor het quantuminnovatie-ecosysteem, maar niet specifiek voor quantumtechnologieën. Daarom gaat deze analyse hier niet verder op in.

135 Voor een systematische review over fundamentele rechten en algoritmen, zie bijvoorbeeld: Gerards, J., et al. (2018). *Algoritmes en grondrechten*. Universiteit Utrecht.

136 Supercomputing is het gebruik van krachtige computersystemen die door middel van grootschalige parallelle verwerking grote hoeveelheden gegevens kunnen verwerken en complexe berekeningen kunnen uitvoeren met een snelheid die de mogelijkheden van conventionele computers overstijgt. In Europees verband wordt hieraan gewerkt via de The European High Performance Computing Joint Undertaking.

137 Lane, B., et al. (2025). *Allocating access to quantum computing: A legal-ethical framework*. QDNL.

138 Zie bijvoorbeeld: Koninklijke Nederlandse Academie van Wetenschappen. (2023). *Kennisveiligheid*.

4.4. Quantumsensing: privacy en gegevensbescherming

Quantumsensoren kunnen de bescherming van fundamentele rechten ondermijnen, met name het recht op privéleven en het recht op bescherming van persoonsgegevens. De toekomst van quantumsensingtechnologieën en de gevolgen daarvan voor bestaande sensing-infrastructuren zijn nog onzeker. Toch is het belangrijk om vanuit het perspectief van *anticipatory governance* al naar mogelijke gevolgen voor fundamentele rechten te kijken. Er zijn veel manieren om quantumsensingtechnologieën toe te passen, met mogelijke gevolgen voor privacy. Daarom gaat deze paragraaf eerst in op die gevolgen door te kijken naar de manier waarop de Europese jurisprudentie over fundamentele rechten van toepassing is op bestaande sensingsystemen. Daarbij is in het bijzonder aandacht voor het recht op privéleven en het recht op bescherming van persoonsgegevens.

Quantumsensing en risico's voor het recht op privéleven

De belangrijkste maatschappelijke zorgen over het gebruik van quantumsensingtechnologieën gaan over privacy, zo blijkt uit wetenschappelijke literatuur en beleidsstukken.[139] Zoals besproken in paragraaf 2.2, kunnen quantumsensoren de prestaties van traditionele sensoren verbeteren en leiden tot nieuwe sensingtoepassingen. Sommige toepassingen kunnen als invasief worden beschouwd. Dat komt door hun vermogen om op afstand heel nauwkeurig zaken te kunnen waarnemen. Dat maakt gegevensverzameling mogelijk die buiten het bereik ligt van klassieke sensoren. Zo kunnen quantumgravimeters privéruimten observeren, ongeacht fysieke belemmeringen, zoals de muren van een huis. Dergelijke toepassingen zouden kunnen zorgen voor meer toezichtsmogelijkheden voor bijvoorbeeld overheden, inlichtingen- en veiligheidsdiensten, opsporingsdiensten en commerciële partijen.

Een andere mogelijke toepassing van quantumsensoren ligt op het gebied van hersenscantechnologie. Daarmee kunnen publieke of private partijen in potentie ongemerkt de hersenactiviteit van een persoon in kaart brengen.[140] Deze technieken vragen om meer aandacht voor zogenoemde 'mentale privacy' en de rol van fundamentele rechten hierbij.[141] De quantummagnetometer is ook een mogelijke toepassing van quantumsensoren. Als bijvoorbeeld drones hiermee uitgerust worden, kunnen personen op afstand gevolgd en

139 Hoofnagle, C. J., & Garfinkel, S. L. (2022). *Law and policy for the quantum age.* Cambridge University Press.
OESO. (2025). An overview of national strategies and policies for quantum technologies. *OECD Digital Economy Papers*.
140 Faccio, D. (2024). The future of quantum technologies for brain imaging. *PLOS Biology*.
141 Ligthart, S. (2026). Mental privacy as part of the human right to freedom of thought? In *The Law and Ethics of Freedom of Thought, Volume 2: Cognitive Liberty, Mental Privacy, and International Law* (pp. 191-215). Springer Nature Switzerland.

geïdentificeerd worden om gegevensverzameling mogelijk te maken.[142] Dit kan aanzienlijke gevolgen hebben voor privacy- en gegevensbescherming, vooral als dergelijke toepassingen gecombineerd worden met andere verzamelde gegevens (bijvoorbeeld elektronische communicatie) en analysemethoden (bijvoorbeeld datawetenschap en AI).

Er spelen veel belangen bij het mogelijke gebruik van quantumsensing. Dit vraagt om strenge beoordelingen door rechters van de rechtmatigheid, proportionaliteit en noodzaak van quantumsensoren, evenals aandacht voor de manier waarop bestaande en opkomende maatschappelijke, politieke en economische krachten de interactie tussen nieuwe technologieën en privacy vormgeven.[143] De volgende paragraaf gaat daarom in op de twee relevante stelsels in Europa voor de bescherming van het recht op privéleven: het EVRM en het Handvest.

Bescherming van het recht op privéleven door het EVRM en Handvest

Het EVRM werd in 1950 in het leven geroepen door de Raad van Europa om mensenrechten en fundamentele vrijheden te beschermen. Alle leden van de Raad van Europa, inclusief alle EU-lidstaten, zijn gebonden aan het EVRM. De beschermingen van het EVRM gelden dus niet alleen voor EU-landen, maar ook voor andere Europese landen die lid zijn van de Raad van Europa. In het Handvest zijn de fundamentele rechten en vrijheden binnen de Europese Unie vastgelegd. Het Handvest geldt voor 'instellingen, organen en instanties van de Unie met inachtneming van het subsidiariteitsbeginsel, alsmede, uitsluitend wanneer zij het recht van de Unie ten uitvoer brengen, tot de lidstaten' (artikel 51). De bescherming van de fundamentele rechten van deze twee stelsels overlapt elkaar. Het Hof van Justitie van de Europese Unie (HJEU), dat het EU-recht en dus het Handvest interpreteert, en het Europees Hof voor de Rechten van de Mens (EHRM), dat het EVRM interpreteert, verwijzen dan ook geregeld naar elkaars jurisprudentie.[144]

Handvest

Artikel 7 van het Handvest voorziet in de bescherming van het recht op privéleven. In artikel 8 is het recht op bescherming van persoonsgegevens vastgelegd, gevolgd door een aantal waarborgen voor de rechtmatige verwerking van persoonsgegevens. Wetten en praktijken die

142 Hoofnagle, C. J., & Garfinkel, S. L. (2022). *Law and policy for the quantum age*. Cambridge University Press.
Škorvánek, I., & Koops, B.-J. (2023). Knowing without entering: How remote police surveillance affects privacy of the home. In *Privacy, Technology, and the Criminal Process*. Routledge.
143 Popelier, P., & Van De Heyning, C. (2013). Procedural rationality: Giving teeth to the proportionality analysis. *European Constitutional Law Review*.
144 Artikel 52. 3 van het Handvest bepaalt dat de betekenis en reikwijdte van de rechten uit het Handvest overeenkomen met die van het Europees Verdrag voor de Rechten van de Mens. Zie bijvoorbeeld ook: Davio, V., & Muir, E. (2023). Introduction. The ECHR in the ECJ's case-law post-charter: A dual perspective. *European Papers - A Journal on Law and Integration*.

artikel 7 en 8 van het Handvest beperken, moeten volgens artikel 52.2 van het Handvest bij wet zijn geregeld en de wezenlijke inhoud van die rechten en vrijheden respecteren. Het recht op privéleven of het recht op de bescherming van persoonsgegevens kan ook worden beperkt vanwege de vrijheid van ondernemerschap die wordt beschermd op grond van artikel 16 van het Handvest.[145]

EVRM

Artikel 8 van het EVRM beschermt personen tegen onrechtmatige inmenging door de staat. Naast de verplichting om een EVRM-recht niet te schenden, bevat dit artikel ook positieve verplichtingen[146] voor landen om de uitoefening van het recht op privéleven te waarborgen. Dit geldt onder andere voor relaties tussen private partijen, zoals commerciële partijen die sensoren gebruiken om personen in de openbare ruimte te monitoren. In het kader van het EVRM kunnen de acties van private partijen alleen indirect worden beoordeeld. Dat gebeurt dan via de verplichting voor de staat om passende maatregelen te treffen om het recht op privéleven van mensen te beschermen in hun contacten met een commerciële entiteit. Denk aan geluidsoverlast door een luchtvaartmaatschappij[147] of een werkgever die de communicatie van een werknemer in de gaten houdt.[148] Elke inmenging met het recht op privéleven moet gelegitimeerd worden volgens de bepalingen van artikel 8.2 van het EVRM.

Interpretatie van het EVRM door het EHRM

Het EHRM verwijst in sommige zaken naar het recht op privéleven in het kader van de toepassing van artikel 8 van het EVRM.[149] Dat doet het op basis van vier pijlers in artikel 8: het recht op privéleven, gezinsleven, woning en correspondentie. Het EHRM behandelt de verwerking van persoonsgegevens als dit binnen de reikwijdte van het begrip 'privéleven' valt. Bij kwesties over de bescherming van persoonsgegevens verwijst het EHRM ook naar Verdrag 108 van de Raad van Europa van 28 januari 1981. Dat verdrag regelt de bescherming van personen bij de geautomatiseerde verwerking van persoonsgegevens ('CETS nr. 108' of 'Verdrag 108', met een protocol bijgewerkt tot Verdrag 108+). Verdrag 108 geldt voor private en publieke partijen. Een belangrijke bijdrage van Verdrag 108+ is dat het ook van toepassing is op

145 Zie ook: Hof van Justitie van de Europese Unie [HJEU]. (2014). *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. Het HJEU oordeelde hierin dat de artikelen 7 en 8 van het Handvest (het recht op privacy en databescherming) zwaarder wegen dan het economische belang van de zoekmachine. Dit geldt specifiek bij een verzoek om zoekresultaten te verwijderen die onjuiste informatie over een bepaald persoon bevatten.

146 Europees Hof voor de Rechten van de Mens [EHRM]. (1979). *Case of Marckx v. Belgium*.

147 EHRM. (2003). *Case of Hatton and Others v. the United Kingdom*.

148 EHRM. (2019). *Case of López Ribalda and Others v. Spain*.

149 EHRM. (2017). *Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*.

gegevensverwerking op het gebied van nationale veiligheid (en defensie). Het Handvest is in beginsel niet van toepassing op dit domein.

Sensingtoepassingen, privacy en gegevensbescherming

Quantumsensoren hebben veelal een dual-use karakter en kennen daarmee zowel toepassingen in het defensie- en veiligheidsdomein als het civiele domein. Zoals besproken, kunnen quantumsensoren met name impact hebben op privacy en gegevensbescherming. In deze paragraaf wordt daarom ingegaan op de relevante wet- en regelgevende kaders voor sensingtoepassingen in deze domeinen, vanuit het perspectief van fundamentele rechten.

Toepassingen in het defensie- en veiligheidsdomein

Momenteel wordt quantumsensing vooral ontwikkeld en toegepast in het defensie- en veiligheidsdomein, voor de uitbreiding van surveillancecapaciteiten. Dat roept de vraag op welke privacy- en gegevensbeschermingsrechten hier gelden.[150] Ten eerste is de AVG in deze domeinen meestal niet van toepassing. Daarnaast vallen defensie en nationale veiligheid grotendeels buiten de reikwijdte van het Unierecht. Dat komt doordat de EU niet bevoegd is op grond van artikel 4.2 van het Verdrag betreffende de Europese Unie. Zo is de bescherming van fundamentele rechten tegen het gebruik van (quantum)sensing niet mogelijk op grond van het Unierecht en valt dit buiten de rechterlijke bevoegdheid van het HJEU. Wel geldt het recht op privéleven op grond van het EVRM. Het EVRM eist dat alle staatsinmenging in fundamentele rechten wordt gerechtvaardigd door een test op de proportionaliteit en noodzaak van die inmenging. Hoe het EHRM de door een staat aangevoerde rechtvaardiging zou beoordelen, is een kwestie van analyse per geval.

Toepassingen in het civiele domein

In een civiele context zouden quantumsensingtoepassingen ingezet kunnen worden om personen beter te kunnen volgen en voor het registreren van mogelijk gevoelige informatie, zoals bij hersenscans. Het EHRM ziet in veel gevallen op grond van artikel 8 van het EVRM dergelijke toepassingen als een inmenging op het recht op privéleven die gerechtvaardigd moet worden.[151]

---

150 Zie bijvoorbeeld: Jansen, R., & Reijneveld, M. (2022). Convention 108+, the GDPR, and Data Processing in the National Security Domain. *European Data Protection Law Review*.

151 EHRM. (2008). *Case of S. and Marper v. the United Kingdom*.
EHRM. (2019). *Case of Catt v. the United Kingdom*.
EHRM. (2019). *Case of López Ribalda and Others v. Spain*.
EHRM. (2003). *Case of Peck vs. the United Kingdom*.
EHRM. (2010). *Case of Uzun v. Germany*.
EHRM. (2021). *Case of Big Brother Watch and Others v. the United Kingdom*.

Bij de beoordeling kijkt het EHRM naar de context waarin de informatie is opgeslagen en bewaard, de aard van de bestanden, de manier waarop ze worden gebruikt en verwerkt en de mogelijke resultaten.[152] Zo ziet het EHRM het verzamelen en bewaren van DNA-profielen als een inbreuk, omdat dit een manier is om genetische verwantschap tussen personen te achterhalen.[153] Het EHRM ziet ook een inbreuk bij het opslaan van videobeelden bij een politiebureau en het gebruik ervan in een strafrechtszaak.[154] Een andere geconstateerde inbreuk is het verzamelen en opslaan van gegevens over de locatie en bewegingen van een persoon in de openbare ruimte door een gps-apparaat dat op diens auto was bevestigd.[155] Het EHRM constateert echter niet standaard dat er sprake is van een schending van het recht op privéleven. De gevolgen van quantumsensingtechnologieën voor fundamentele rechten moet worden bezien in het licht van deze beginselen, met aandacht voor de specifieke kenmerken van elke casus.

Het EVRM en het Handvest verbieden toezicht en gegevensverzameling met sensoren niet per definitie. Het monitoren en verzamelen van informatie met behulp van sensoren worden beschouwd als een overheidstaak. Er zijn echter wel waarborgen nodig tegen misbruik. Wanneer er sprake is van een inmenging in het recht op privéleven moeten landen de noodzaak hiervan aantonen en dit toespitsen op het belang voor de democratische rechtsorde – normen die strikt door rechtbanken worden geïnterpreteerd als het gaat om het beperken van fundamentele rechten. Ongerichte grootschalige informatieverzameling over personen zal de proportionaliteitstoets waarschijnlijk niet doorstaan. Dit roept vragen op over de technische en wettelijke voorwaarden voor het toestaan van gerichte informatieverzameling. Het is onzeker of er quantumsensingtoepassingen ontworpen kunnen worden om gericht informatie te verzamelen. In laboratoriumonderzoek passen onderzoekers hersenscantechnologie toe bij zorgvuldig geselecteerde deelnemers in lijn met de ethische uitgangspunten voor medisch onderzoek. Dat is heel anders dan het op grote afstand observeren van personen, auto's, of huizen in de openbare ruimte.

152 EHRM. (2008). *Case of S. and Marper v. the United Kingdom*.

153 Ibid.

154 EHRM. (2003). *Case of Perry v. the United Kingdom*.

155 EHRM. (2010). *Case of Uzun v. Germany*.

De verzameling van persoonsgegevens kan, naast het recht op privéleven, bovendien ingrijpende gevolgen hebben voor het uitoefenen van de vrijheid van meningsuiting en vergadering.[156] Daarnaast kan onrechtmatige informatieverzameling door overheidsinstanties vragen oproepen tijdens strafrechtelijk onderzoek, vooral over het recht op een eerlijk proces.[157]

Het is goed mogelijk dat bepaalde toepassingen van quantumsensoren moeten worden getoetst aan de bescherming die artikel 8 van het EVRM biedt tegen massasurveillance. Toepassingen van quantumsensing kunnen in het bijzonder inbreuk maken op privacy vanwege hun vermogen om verschijnselen op afstand te detecteren. Individuen zouden zich er bovendien vaak niet van bewust zijn dat zij door middel van quantumsensoren worden geobserveerd. Daarnaast hoeft surveillance door middel van sensing niet rechtstreeks op een specifiek individu te zijn gericht. De jurisprudentie over artikel 8 maakt het mogelijk om de rechtmatigheid van surveillancepraktijken met sensoren alleen te beoordelen wanneer een sensorsysteem gericht is op een specifiek persoon.[158]

Om onderzoek te kunnen doen naar massasurveillance, zijn volgens juristen de eisen voor personen om een vordering te kunnen indienen een al langer bestaand probleem.[159] Hiervoor moeten mensen namelijk aantonen dat zij slachtoffer zijn geweest van een inbreuk op het EVRM op grond van artikel 34. Het kan voor burgers lastig zijn om een schending van hun recht op privéleven aan te tonen, vooral als zij ongemerkt gevolgd worden. Daarom heeft het EHRM de weg vrijgemaakt voor artikel 8-onderzoek naar massasurveillance zonder bewijs van een directe inbreuk. Uit de beslissing van het EHRM in de zaak Roman Zakharov versus Rusland volgt dat een verzoeker kan stellen slachtoffer te zijn van een schending, puur omdat geheime surveillancemaatregelen bestaan, of wetgeving die deze maatregelen toestaat.[160] Hieraan wordt voldaan wanneer de verzoeker mogelijk getroffen is door de surveillancemaatregel en er effectieve rechtsmiddelen bestaan tegen mogelijke privacyschendingen.[161] Dit laat volgens experts echter nog te veel ruimte voor landen. Dat komt doordat mensen nog steeds slechts kunnen vermoeden dat ze getroffen zijn door geheime surveillancemaatregelen.[162]

---

156 EHRM. (2023). *Case of Glukhin v. Russia*.

EHRM. (2019). *Case of Catt v. the United Kingdom*.

157 Škorvánek, I., & Koops, B.-J. (2023). Knowing without entering: How remote police surveillance affects privacy of the home. In ***Privacy, Technology, and the Criminal Process***. Routledge.

158 EHRM. (2010). *Case of Uzun v. Germany*.

159 Kosta, E. (2022). Algorithmic state surveillance: Challenging the notion of agency in human rights. *Regulation & Governance*.

160 EHRM. (2015). *Case of Roman Zakharov v. Russia*.

Zie ook: Kosta, E. (2022). Algorithmic state surveillance: Challenging the notion of agency in human rights. *Regulation & Governance*..

161 Ibid.

162 Kosta, E. (2022). Algorithmic state surveillance: Challenging the notion of agency in human rights. *Regulation & Governance*.

Quantumsensing ter bevordering van het recht op privéleven

Ontwikkelingen in nieuwe sensingtechnologieën bieden ook de mogelijkheid om het recht op privéleven juist te versterken. Het toepassen van quantumsensing kan worden gezien als een maatregel die landen kunnen of moeten nemen om het uitoefenen van het recht op privéleven te waarborgen ('positieve verplichtingen').[163] Met quantumsensing kunnen bijvoorbeeld veranderingen in het klimaat gemeten worden.[164] Uit artikel 8 van het EVRM volgen verplichtingen om de leefomgeving van personen te beschermen. Een gezond milieu en klimaat worden daarbij gezien als factoren die kunnen bijdragen aan welzijn en kwaliteit van leven.[165] Volgens het Verdrag van Aarhus,[166] waarvan de EU ondertekenaar is, is de beschikbaarheid en toegankelijkheid van milieu-informatie een kernonderdeel om deel te kunnen nemen aan besluitvorming over milieu. Dit verdrag verplicht ondertekenaars daarom om milieu-informatie beschikbaar te stellen aan het publiek en overheidsinstellingen.

Bij zaken over milieubescherming op grond van artikel 8 verwijst het EHRM naar het belang van milieu-informatie.[167] Het EHRM kijkt hierbij onder andere naar het soort beleid of besluit, de mate waarin rekening is gehouden met de standpunten van personen tijdens het besluitvormingsproces en de procedurele waarborgen.[168] Het EHRM onderzoekt daarom de publieke bekendheid van activiteiten die gevolgen hebben voor het leefmilieu van mensen, om zo de mogelijke risico's en effecitiviteit van oplossingen te kunen beoordelen. Verder zijn de omvang, kwaliteit en interpretatie van de met sensoren verzamelde informatie belangrijk om vast te stellen wat precies de zorgplicht en de bewijsnorm voor milieubescherming van de overheid is. In kwesties waarbij wetenschappelijke onzekerheden bestaan, zoals de klimaatcrisis, zorgt het voorzorgsbeginsel voor omkering van de bewijslast. Dit is een van de beginselen van het internationale recht en het milieurecht.[169] Het verplicht entiteiten die mogelijk schadelijke activiteiten ondernemen om voorafgaand aan de activiteit potentiële milieurisico's te onderbouwen op basis van wetenschappelijk bewijs.

---

163 Zeybek, B. (2026). What environmental sensing means for the scope of the right to private life. *Law, Innovation and Technology*.

164 Berger, C., et al. (2021). Quantum technologies for climate change: Preliminary assessment. *arXiv*.

165 EHRM. (2024). *Case of Verein Klimaseniorinnen Schweiz and Others v. Switzerland*.

166 De officiële naam is het Verdrag betreffende toegang tot informatie, inspraak bij besluitvorming en toegang tot de rechter inzake milieuaangelegenheden. Het verdrag valt onder UNECE, de Europese economische commissie van de Verenigde Naties. Het verdrag is in de EU geïmplementeerd via Richtlijn 2003/4/EG inzake de toegang van het publiek tot milieu-informatie. Zie: United Nations Economic Commission for Europe. (1998). *Convention on access to information, public participation in decision-making and access to justice in environmental matters*.

167 EHRM. (2009). *Affaire Tatar v. Romania*.

168 EHRM. (2004). *Case of Taşkin and Others v. Turkey*.

169 De Sadeleer, N. M. (2010). The precautionary principle in EU law. *Aansprakelijkheid, Verzekering En Schade*.

Het EHRM stelt geen specifieke vereisten aan sensortechnologiëen. Quantumsensoren zouden echter noodzakelijk kunnen worden voor landen om de verplichtingen na te komen op het gebied van milieu-informatie op grond van artikel 8. Dat zou met name gelden voor toepassingen voor de meting van klimaat- en milieufactoren. Vanuit een grondrechtelijk perspectief is het verzamelen van gegevens met sensoren niet alleen nodig om democratische participatie bij besluitvorming over het milieu te vergemakkelijken, maar ook voor het produceren en beoordelen van wetenschappelijk bewijs.

Verder is er in de EU strenge regulering voor het civiele gebruik van sensingtechnieken in de openbare ruimte. De specifieke eisen hangen af van de plaatsing van de camera of sensor en het doel van het gebruik ervan. Het maakt bijvoorbeeld uit of het om tijdelijke of reguliere detectie gaat.[170] Elk gebruik van sensingtechnieken door bedrijven en overheidsinstanties[171] waarmee mogelijk personen te identificeren zijn, komt neer op de verwerking van persoonsgegevens en moet voldoen aan de AVG. Deze toepassingen moeten een juridische grondslag hebben en moeten worden gebruikt op een wijze die evenredig is aan het doel waarvoor zij worden ingezet. Juridische grondslagen kunnen worden gevonden in wetgeving die betrekking heeft op lokale overheden, zoals de Gemeentewet, en zijn gebaseerd op een gerechtvaardigd belang. Bij cameratoezicht door overheden in de openbare ruimte is bijvoorbeeld de openbare veiligheid of het opsporen of voorkomen van criminele activiteiten een gerechtvaardigd belang. Daarnaast vereist het noodzakelijkheidsbeginsel dat cameratoezicht de enige aannemelijke optie is voor de specifieke verwerkingsdoeleinden.[172] Toegang tot en gebruik van deze gegevens door rechtshandhavingsinstanties moeten voldoen aan de Richtlijn gegevensbescherming bij rechtshandhaving. Gerechtvaardigde belangen kunnen op grond van het Handvest alleen worden gebruikt om de rechten op privéleven en bescherming van persoonsgegevens te beperken als dit proportioneel is ten opzichte van de aard, ernst en het doel van de inbreuk. Ook moet de inbreuk worden beperkt tot het strikt noodzakelijke.

Quantumsensing en de bescherming van fundamentele rechten

Tot op heden zijn er nog geen commerciële en grootschalige toepassingen van quantumsensing, maar alleen kleinschalig gebruik in enkele strategische sectoren. Daarom is het de vraag hoe het

170 Zie bijvoorbeeld voor videosurveillance: HJEU. (2014). *František Ryneš v. Úřad pro ochranu osobních údajů*.

171 Dit geldt niet voor defensie, nationale veiligheid en rechtshandhaving.

172 EU-Hof. (2014). *Case of Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*.

recht op privéleven effectief kan worden beschermd bij een techniek waarvan het toekomstige gebruik onduidelijk is. Bepaalde soorten quantumsensoren brengen in potentie ernstige privacyrisico's met zich mee. De noodzaak voor het rechtstelsel om deze risico's te ondervangen ontstaat waarschijnlijk pas als de toepassingen ook echt gebruikt worden in de praktijk. Europa heeft een zeer robuust technologieneutraal wettelijk stelsel voor de effectieve bescherming van de rechten op privéleven en de bescherming van persoonsgegevens door middel van waarborgen van fundamentele rechten en specifieke wetgeving, zoals de AVG, waardoor privacyrisico's als gevolg van quantumtechnologie in ieder geval al deels worden afgedekt.

Wanneer er geen consensus is over de ontwikkeling van nieuwe technologieën die het privéleven schenden, verwacht het EHRM van een lidstaat die een 'pioniersrol' op het gebied van quantumtechnologie opeist, om 'bijzondere verantwoordelijkheid te dragen om de juiste balans te bereiken' tussen de inzet van nieuwe technologie en de bescherming van privacy.[173] Als de gevolgen voor privacy niet van tevoren vast te stellen zijn, kunnen beleidsmakers hun toevlucht nemen tot het voorzorgsbeginsel, dat al werd genoemd in de vorige subparagraaf.[174] Dit is een aanbevolen aanpak om de maatschappelijke gevolgen van nieuwe technologieën te ondervangen, inclusief risico's voor privacy.[175]

Het blijft onzeker in hoeverre de besproken gevolgen voor privacy werkelijkheid worden door het toepassen van quantumsensoren. Quantumsensingtechnologieën zijn op dit moment alleen commercieel aantrekkelijk voor zeer specifieke sectoren, zoals biogeneesmiddelen en het in kaart brengen van de ondergrondse infrastructuur. Het lijkt onwaarschijnlijk dat in consumentenapparatuur quantumsensoren worden ingebouwd, vanwege de hoge kosten en de nu nog slechte prestaties. Zelfs als deze in de toekomst beter worden, bieden ze niet meteen meerwaarde. Er bestaan immers al goed presterende klassieke sensoren. Vanuit het perspectief van fundamentele rechten en *anticipatory governance* kunnen toekomstige acties zich richten op de verbetering van de beoordeling van de proportionaliteit van fundamentele rechten in de hele productcyclus, dus van ontwikkeling tot toepassing van nieuwe sensingtechnieken. Dat is belangrijk om de gelijke toegang tot sensingcapaciteiten te waarborgen, verantwoordings- en

173 EHRM. (2008). *Case of S. and Marper v. the United Kingdom*.
EHRM. (2017). *Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*.
174 Kegge, R. (2020). The precautionary principle and the burden and standard of proof in European and Dutch environmental law. *Review of European Administrative Law*.
Europese Commissie. (2000). *Communication from the Commission on the Precautionary Principle*.
175 European Data Protection Supervisor. (2019). *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*.

transparantiemechanismen in de gehele waarde- en toeleveringsketen te integreren, en voor de democratische toetsing van de surveillancecapaciteit van digitale infrastructuren.[176]

4.5. Waarborging van fundamentele rechten op de lange termijn

Van oudsher bestaat de bescherming van fundamentele rechten uit verschillende aspecten. Zo gaat het om de verhouding tussen de staat en de individuele burger. Fundamentele rechten beschermen de bevolking tegen schendingen door de staat, zoals massasurveillance met behulp van nieuwe sensingtechnologieën. In een democratische samenleving moet elke inmenging die de uitoefening van fundamentele rechten beïnvloedt noodzakelijk zijn. Burgers kunnen de rechter inschakelen als dat niet het geval is.

Bescherming van fundamentele rechten heeft ook een positievere kant, die actieve betrokkenheid van de staat vereist. Staten, waaronder Nederland, zijn verplicht het daadwerkelijke uitoefenen van fundamentele rechten te waarborgen, ook tussen personen onderling en tussen personen en technologiebedrijven. Daar hebben staten verschillende instrumenten voor. Zo helpen wetten op het gebied van gegevensbescherming om de bescherming van fundamentele rechten te waarborgen bij het verwerken van persoonsgegevens. En de e-privacyrichtlijn en de Telecommunicatiewet helpen het recht op geheimhouding van communicatie te beschermen. Voor de bescherming van de fundamentele rechten van gebruikers van sociale media en andere online platforms is er bijvoorbeeld de Digitaledienstenverordening (DSA). Hoewel deze verordening niet gericht is op quantumtechnologie, beschermt ze de vrijheid van meningsuiting, privacy, gegevensbescherming, consumentenbescherming en het recht op non-discriminatie. Wetten die de toepassing eisen van quantumveilige encryptiemaatregelen kunnen ook worden gezien als instrumenen die door staten ingezet worden om fundamentele rechten te beschermen.

Digitale soevereiniteit

Het debat over digitale soevereiniteit laat zien dat het vermogen van landen om digitale infrastructuren en bijbehorende diensten effectief te reguleren vanuit het oogpunt van fundamentele rechten niet vanzelfsprekend is. Een van de belangrijkste redenen voor de aandacht voor digitale soevereiniteit op Europees en nationaal niveau is dan ook het vermogen

176 Zie ook: Hayes, B. (2012). *The surveillance-industrial complex. In Routledge handbook of surveillance studies* (pp. 167–175). Routledge.

van landen om daadwerkelijk invloed uit te oefenen op de wijze waarop nieuwe digitale technologieën in de samenleving worden ingezet en uiteindelijk gevolgen hebben voor de uitoefening van fundamentele rechten.

De zorgen die hierover bestaan, hebben onder andere geleid tot de focus op digitale soevereiniteit op Europees en nationaal niveau. Door geopolitieke ontwikkelingen staat digitale soevereiniteit hoog op de agenda in EU-debatten. Tijdens de zittingsperiode van de vorige Europese Commissie werd het benoemd tot kerndoel. Sinds 2024 is digitale soevereiniteit een kernverantwoordelijkheid van de uitvoerend vicevoorzitter voor Technologische Soevereiniteit, Veiligheid en Democratie. Voor de bescherming van fundamentele rechten is het belangrijk dat de agenda voor digitale soevereiniteit blijft aansluiten bij de bescherming van de fundamentele waarden van de EU, waaronder de rechten die zijn vastgelegd in het Handvest en EVRM.

In EU-beleidsdebatten over digitale soevereiniteit komen quantumtechnologieën veel aan de orde. Daarnaast erkennen EU-beleidsstukken de wereldveranderende potentie van quantumtechnologieën, maar is er tegelijkertijd waarkzaamheid vanwege hun mogelijke disruptieve invloed.[177] Digitale soevereiniteit wordt in de bredere EU-context gebruikt voor een breed scala aan beleidsdoelstellingen over de ontwikkeling en het gebruik van digitale technologieën, waarbij aanzienlijke gevolgen voor fundamentele rechten kunnen ontstaan. Hieronder valt de noodzaak om opnieuw zeggenschap te verkrijgen over data, infrastructuren en (kritieke) technologieën. Ook erkent de EU het belang van strategische autonomie, samenwerking met geopolitieke bondgenoten en het terugdringen van kritieke afhankelijkheden. De EU stelt dat het essentieel is om onafhankelijk op te treden in de digitale wereld, omdat dit een belangrijke manier is om onze waarden te beschermen.

177 Voor een bespreking, zie: Vogiatzoglou, P. (2025). The EU's quest for digital sovereignty: A matter of quantum innovation? *Digital Society*. Zie ook: Vogiatzoglou, P., & Van Hoboken, J. (te verschijnen). The EU's digital sovereignty and quantum technologies: To what end? *Law, Innovation and Technology*.

5. Aanbevelingen

Quantumtechnologie kan verschillende gevolgen hebben voor de maatschappij. Dit deel ging in op de gevolgen die quantumtechnologieën in het algemeen en bepaalde quantumtoepassingen in het bijzonder kunnen hebben voor publieke waarden en fundamentele rechten. De besproken ethische en juridische perspectieven vormen samen elementen van *anticipatory governance*. Deze benadering heeft als doel om de uitdagingen en kansen van quantumtechnologie aan te pakken op het moment dat ze zich voordoen. Zo kunnen beleidsmakers en besluitvormers flexibel reageren op snelle ontwikkelingen, en is er ruimte om beslissingen te nemen die bijdragen aan publieke waarden en de bescherming van fundamentele rechten. Dat is essentieel in de context van quantumtechnologie, omdat er nog veel onzekerheden zijn. Dit hoofdstuk geeft twee aanbevelingen:

1. Zorg voor continue, grondige monitoring van de ontwikkelingen op het gebied van quantumtechnologie.
2. Wees bereid om te handelen op basis van relevante publieke waarden en de mogelijke gevolgen voor fundamentele rechten.

Continue en grondige monitoring van ontwikkelingen

Quantumtechnologie bevindt zich nog in een vroeg stadium. Het is daarom essentieel dat beleidsmakers en besluitvormers op de hoogte blijven van relevante ontwikkelingen. Dat geldt zowel voor mogelijke nieuwe toepassingen als voor de gevolgen voor relevante publieke waarden en wet- en regelgeving. Het is daarom van belang dat stakeholders die bij quantuminnovatie betrokken zijn constant informatie delen over technologische ontwikkelingen en doorbraken.

De mogelijke negatieve gevolgen voor publieke waarden zijn in deze analyse al deels in beeld gebracht. Daarom kan hierop nu al gehandeld worden. Denk aan het opstellen van vereisten voor inclusie en participatie in maatschappelijke besluitvorming over quantumtechnologieën. En aan het creëren van maatschappelijke bewustwording, bijvoorbeeld over de algoritmemaatschappij en de risico's die dit meebrengt voor rechtvaardigheid en menselijke integriteit. Ook moet er aandacht zijn voor democratie en democratisering en voor overwegingen omtrent openheid en geslotenheid in het kader van strategische autonomie.

Vanuit het perspectief van de bescherming van fundamentele rechten zijn er twee belangrijke problemen die nu moeten worden aangepakt. Dat gaat ten eerste om de gevolgen voor communicatie- en informatieveiligheid door de ontwikkelingen in quantumcomputing. Het tweede probleem is de bescherming van privacy bij het toepassen van quantumsensing. Meer in het algemeen zijn in het rapport de relevante wet- en regelgevingsinstrumenten besproken die kunnen helpen bij het waarborgen van fundamentele rechten zodra bepaalde quantumtechnologieën en -toepassingen tot stand komen en ingezet gaan worden.

Handelen op basis van relevante publieke waarden en mogelijke gevolgen voor fundamentele rechten

Wees alert en bereid om te handelen. Dat is essentieel om goed om te gaan met de mogelijke voordelen en risico's van quantumtechnologieën voor de Nederlandse samenleving. Veel problemen bij de ontwikkeling van quantumtechnologie zijn niet anders dan de problemen bij andere nieuwe en opkomende technologieën. Toch is er ook een belangrijk verschil. Quantumtechnologie krijgt geopolitiek bijzonder veel aandacht, terwijl er nog vrijwel geen concrete toepassingen van quantum bestaan.

Er moeten besluiten worden genomen over de rol van quantumtechnologieën voor de Nederlandse samenleving, en over het belang van publieke waarden en fundamentele rechten in het bredere innovatiebeleid. In een constitutionele democratie als Nederland vormen fundamentele rechten harde grenzen bij de ontwikkeling van nieuwe technologieën. Zo zijn het recht op privéleven en het recht op bescherming van persoonsgegevens vereisten die altijd in acht genomen moeten worden, bij welke technologie dan ook.

Aan de andere kant zijn er genuanceerde beslissingen te maken over publieke waarden, en hoe quantumtechnologie kan leiden tot positieve resultaten voor de maatschappij. *Quantum for good* kan worden gezien als een kernprincipe voor de ontwikkeling van quantumtechnologie. Daarbij zijn er meerdere betekenissen van 'goed' mogelijk.[178] Zo kan het 'goede' worden benadrukt op het gebied van de economie en nationale veiligheid. Het 'goede' kan echter ook gaan over het faciliteren van welvaart of sociale zekerheid. Deze verschillende vormen sluiten elkaar uiteraard niet uit, maar ze houden wel andere resultaten in. In het eerste geval gaat het vooral om economische en defensie-ambities voor de samenleving, in het tweede om het belang van een

178 De Jong, E., & Shelley-Egan, C. (2026). Quantum for good through a lens of technosolutionism. A critical-constructive view. *Journal of Responsible Technology*.

verantwoorde inbedding van quantumtechnologieën in de samenleving. Er zijn dus belangrijke besluiten en compromissen nodig. Hierover moet niet alleen worden beslist vóór de samenleving, maar ook mét de samenleving. Nederland is daarnaast een belangrijke speler in de Europese Unie en in andere internationale gremia. Daarom is het belangrijk dat Nederland trouw blijft aan zijn streven naar strategische autonomie. Dat zorgt enerzijds voor openheid naar de wereld, en betekent anderzijds een verankering van Nederlands sterke positie op het gebied van waardegedreven innovatie.

Deel 2:

Quantumtechnologie in de praktijk

Quantumtoepassingen en publieke waarden

De impact van technologie op publieke waarden is grotendeels afhankelijk van de specifieke context waarin de technologie wordt toegepast. Dit geldt ook voor quantumtechnologie. Om beter te begrijpen hoe publieke waarden in de praktijk een rol spelen bij quantumtechnologie, is het waardevol om deze vraagstukken te verkennen aan de hand van concrete toepassingen. Door mogelijke effecten, betrokken actoren en onderliggende waarden vroegtijdig te verkennen, worden aanknopingspunten zichtbaar om te anticiperen op de impact van quantumtechnologie op de maatschappij.

Daarom biedt dit deel een verkenning van de mogelijke impact van een toepassing van quantumtechnologie. Hiervoor is gebruikgemaakt van het *Exploratory Quantum Technology Assessment* (EQTA) van het Centre for Quantum and Society van QDNL. Eerst wordt ingegaan op de EQTA-methodiek. Vervolgens komen inzichten uit een EQTA-workshop aan bod. Hierbij illustreert een concrete casus hoe publieke waarden betekenis krijgen binnen een specifiek toepassingsgebied van quantumtechnologie. De slotparagraaf geeft op basis van deze inzichten een reflectie en analyse vanuit het perspectief van publieke waarden en beleidsrelevantie.

De EQTA-methodiek

De EQTA-methodiek is ontwikkeld met het uitgangspunt dat quantumtechnologie een sleuteltechnologie is met potentieel grote maatschappelijke impact, terwijl veel toepassingen nog in ontwikkeling zijn en hun precieze implicaties onzeker zijn. Door in een vroeg stadium na te denken over mogelijke kansen en risico's, kunnen organisaties mogelijke ongewenste effecten herkennen en voorkomen. Tegelijkertijd kunnen ze de randvoorwaarden scheppen om de mogelijkheden van quantumtechnologie op een verantwoorde manier te benutten.

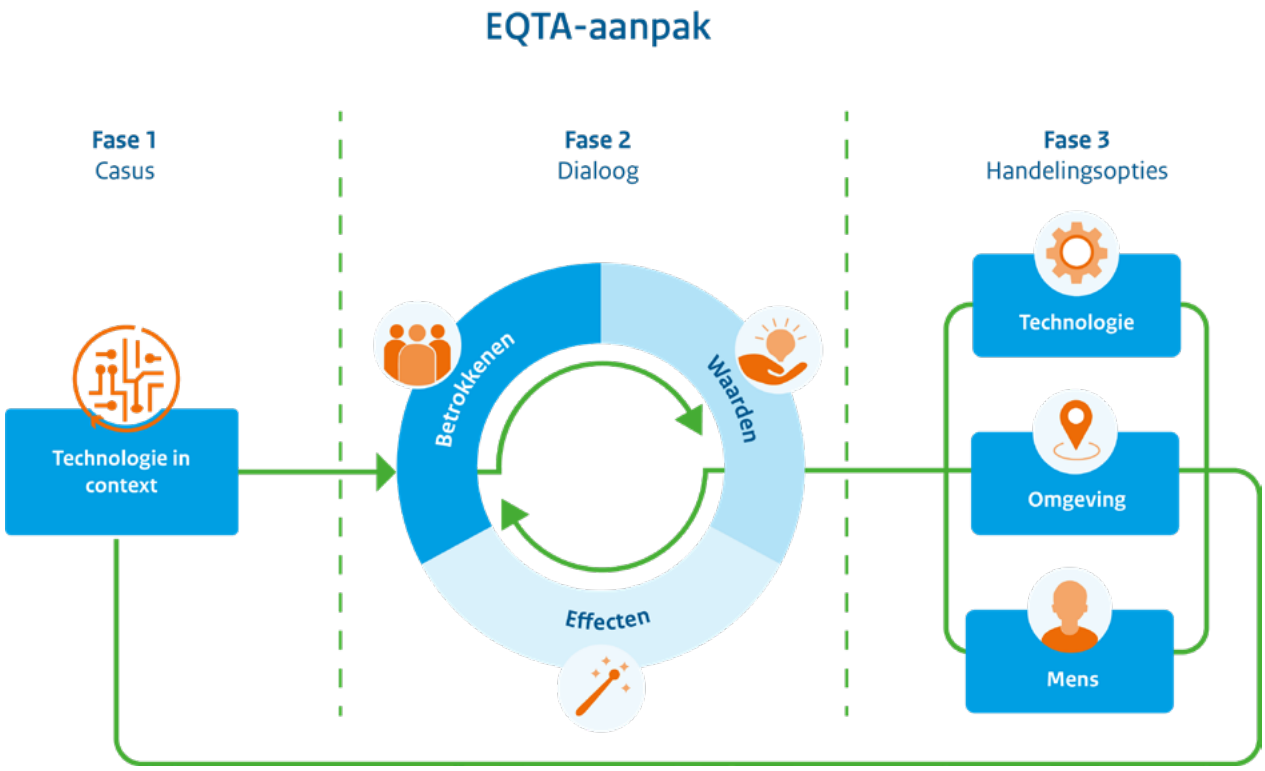
Deelnemers verkennen met de EQTA-methodiek de mogelijke impact van een toepassing van quantumtechnologie (zie figuur 1). De deelnemers bestaan uit technologische experts, beleidsmakers en andere betrokken stakeholders. Ze verkennen de mogelijke impact in drie fasen. In de eerste, verkennende fase kijken ze naar de technologische ontwikkeling en mogelijke toepassingsmogelijkheden, gevolgd door een analyse van relevante stakeholders en

de mogelijke impact van de technologie op organisaties en hun omgeving. Vervolgens onderzoeken ze maatschappelijke, technische, juridische en ethische kaders die van belang zijn voor de toepassing van de technologie.

Een belangrijk onderdeel van de methode is de dialoog met stakeholders. Dit is de tweede fase. Tijdens deze dialoog brengen deelnemers gezamenlijk in kaart welke actoren betrokken zijn, welke positieve en negatieve effecten kunnen optreden en welke waarden daarbij een rol spelen. Deze dialoog maakt het mogelijk om verschillende perspectieven en belangen samen te brengen en om gezamenlijk te reflecteren op de mogelijke maatschappelijke implicaties van technologische ontwikkeling.

Op basis van deze analyse verkennen de deelnemers in fase drie de handelingsopties. Deze handelingsopties kunnen gaan over het ontwerp van de technologie zelf, over de manier waarop mensen met de technologie werken, of over organisatorische of institutionele randvoorwaarden (zoals beleid, regelgeving of samenwerking). Door deze opties expliciet te maken, kunnen organisaties beter afwegen welke stappen nodig zijn om publieke waarden te beschermen.

Figuur 1 De drie fasen in een EQTA-workshop



Bron: Centre for Quantum and Society

Casus: OPM-MEG-helm met quantumsensoren in Amsterdam UMC

Technologie en context van de casus

In deze EQTA-workshop is verkend hoe quantumsensoren kunnen worden toegepast voor het meten van hersenactiviteit in de zorg. De casus[179] richt zich op magneto-encefalografie (MEG), een techniek om magnetische signalen van de hersenactiviteit te meten. Traditionele MEG-systemen maken gebruik van grote scanners, in een afgeschermde ruimte, terwijl deze nieuwe systemen veel kleiner en praktischer van formaat zijn.

In de workshop bespraken vijftien deelnemers uit het bedrijfsleven, de Rijksoverheid, toezichthoudende organisaties, universiteiten, en kennisinstellingen hoe quantumsensoren, zogenoemde *optically pumped magnetometers* (OPM's), kunnen worden toegepast in een helm die om het hoofd van de patiënt wordt geplaatst. Deze sensoren maken gebruik van quantummechanische eigenschappen van atomen. Daardoor kunnen extreem kleine magnetische velden worden gemeten die ontstaan door elektrische activiteit in de hersenen. In de helm zijn meerdere van deze sensoren geïntegreerd. Deze technologie kan hersenactiviteit nauwkeuriger en flexibeler registreren dan traditionele systemen, omdat de sensoren dichter bij de hersenen geplaatst kunnen worden. Tegelijkertijd kunnen patiënten zich tijdens de meting vrijer bewegen. De deelnemers bespraken dat deze ontwikkeling nieuwe mogelijkheden kan bieden voor diagnostiek en onderzoek naar hersenaandoeningen, zoals epilepsie. Dit kan de behandeling van patiënten verbeteren.

Koppeling met publieke waarden

Uit de workshop blijkt dat innovatieve quantumsensoren nieuwe mogelijkheden kunnen bieden voor het meten en analyseren van hersenactiviteit. Het gebruik van dergelijke technologie roept ook vragen op, bijvoorbeeld over de omgang met medische gegevens en de interpretatie en toepassing daarvan in de zorgpraktijk. Het meten van hersenactiviteit genereert gevoelige medische informatie. Daarom zijn het gebruik en de bescherming van gegevens belangrijke aandachtspunten in de verdere ontwikkeling en toepassing van de technologie.

Vanuit het perspectief van publieke waarden raakt deze toepassing met name aan privacy. Hersendata behoren tot de meest gevoelige medische gegevens. Het verzamelen en analyseren van dergelijke data roept vragen op over hoe deze gegevens worden opgeslagen, beschermd en

179 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, QDNL, & Amsterdam UMC. (2025). *Verslag EQTA OPM-MEG. Quantum in de gezondheidszorg*.

gebruikt in diagnostische besluitvorming. Daarnaast spelen rechtvaardigheid, inclusie en participatie een rol bij vragen over toegang tot nieuwe diagnostische technologie en de verdeling van zorgmiddelen. Zo is het mogelijk dat deze technologie in eerste instantie alleen beschikbaar is in gespecialiseerde zorginstellingen. Dit roept de vraag op wie bepaalt welke patiënten toegang krijgen. De casus raakt ook aan de publieke waarde democratie, vooral als het gaat om de manier waarop besluitvorming plaatsvindt en welke partijen daarbij betrokken zijn. Dit kan van invloed zijn op het vertrouwen van patiënten en burgers in de inzet van deze technologie.

Deze casus laat zien dat quantumsensoren in de zorg niet alleen nieuwe technologische mogelijkheden bieden, maar ook vragen oproepen over de manier waarop gevoelige data worden beschermd, hoe toegang tot nieuwe technologie wordt georganiseerd en hoe transparantie over het gebruik en de besluitvorming kan worden geborgd.

Handelingsopties

De casus van Amsterdam UMC illustreert hoe publieke waarden concreet naar voren kunnen komen in een toepassing van quantumtechnologie. Hoewel het om één specifieke toepassing gaat, kunnen de vraagstukken ook relevant zijn voor andere domeinen waarin quantumsensoren worden toegepast. De volgende handelingsopties zijn gebaseerd op de inzichten uit de workshop. In deze EQTA-sessie hebben experts en stakeholders mogelijke kansen, risico's en aandachtspunten voor publieke waarden verkend.

Databeheer

De casus illustreert dat het verzamelen en analyseren van data een centrale rol speelt bij de toepassing van quantumsensoren. Het meten van hersenactiviteit genereert gevoelige medische informatie, wat vragen oproept over opslag, gebruik en bescherming van gegevens. Dit raakt aan de publieke waarde privacy, met name in relatie tot transparantie over hoe data worden gebruikt in diagnostische besluitvorming en hoe ze worden gedeeld binnen zorgsystemen. Wanneer dergelijke technologie breder wordt toegepast, kunnen er onduidelijkheden ontstaan over databeheer, eigenaarschap van data en verantwoordelijkheden rond datagebruik. Dit kan risico's met zich meebrengen voor de bescherming van gevoelige gegevens en voor transparantie richting burgers.

Mogelijke handelingsopties voor verdere beleidsontwikkeling:

- Duidelijke richtlijnen ontwikkelen voor databeheer, gegevensbescherming en bewaartermijnen bij nieuwe innovaties met quantumsensoren.
- Duidelijke rollen, verantwoordelijkheden en autorisatie vastleggen voor toegang tot gevoelige data.
- Transparantie en communicatie stimuleren over de verzameling, interpretatie en het gebruik van data.
- Systemen cyberveilig ontwerpen en onderhouden, gericht op bescherming tegen datalekken en aanvallen.

Toegankelijkheid

Nieuwe technologie is in eerste instantie vaak alleen beschikbaar binnen specifieke instellingen, zoals gespecialiseerde ziekenhuizen. Dit kan leiden tot verschillen in toegang tot innovatieve diagnostiek tussen patiëntgroepen of regio's. Nieuwe diagnostische technologie kan namelijk invloed hebben op hoe patiënten worden onderzocht en behandeld. Dit raakt aan de publieke waarden rechtvaardigheid, inclusie en participatie, en sluit aan bij bredere vraagstukken rond de verdeling van technologische capaciteit en kennis. Tijdens de workshop bespraken deelnemers dat er ongelijkheid in de toegang tot effectieve zorg kan ontstaan wanneer dergelijke technologie breder wordt toegepast. Ook kan het leiden tot verschillen in beschikbare kennis, technische infrastructuur en capaciteit tussen organisaties die verantwoordelijk zijn voor de monitoring van vitale infrastructuren.

Mogelijke handelingsopties voor verdere beleidsontwikkeling:

- Toegankelijkheid monitoren van quantuminnovaties binnen publieke voorzieningen.
- Brede toegankelijkheid tot toepassingen van quantumtechnologie stimuleren, in het bijzonder in publieke diensten.
- Richtlijnen en standaarden ontwikkelen voor toepassing van quantumtechnologie in de zorg en infrastructuur.
- Inzetten op werving, opleiding en training van professionals die met deze technologieën kunnen werken.

Maatschappelijke legitimiteit en besluitvorming

De casus toont aan dat de toepassing van quantumsensoren niet alleen over technische keuzes gaat, maar ook vraagt om afstemming tussen verschillende stakeholders, zoals zorginstellingen, onderzoekers, beleidsmakers en patiënten. Door in een vroeg stadium na te denken over

mogelijke toepassingen en implicaties, kan beter worden voorbereid op toekomstige inzet van deze technologie. Dit benadrukt het belang van transparante en verantwoorde besluitvorming en raakt daarmee aan de publieke waarde democratie, in het bijzonder waar het gaat om publieke verantwoording en betrokkenheid bij technologische ontwikkeling. Tegelijkertijd benadrukten deelnemers aan de workshop dat technologische ontwikkeling vaak plaatsvindt in specialistische omgevingen, waardoor besluitvorming zich kan concentreren bij een beperkte groep experts of organisaties. Dit vraagt om extra aandacht voor transparantie en maatschappelijke betrokkenheid bij de ontwikkeling en toepassing van dergelijke technologieën.

Mogelijke handelingsopties voor verdere beleidsontwikkeling:

- Dialoog tussen technologische experts, beleidsmakers en maatschappelijke stakeholders faciliteren over mogelijke toepassingen van quantumtechnologie.
- Transparante en heldere communicatie over de technologische toepassingen richting de eindgebruikers stimuleren.
- Kaders voor publieke verantwoording en toezicht bij de toepassing van quantum innovaties stimuleren.
- Methoden als de EQTA benutten om de maatschappelijke implicaties van quantumtechnologie te verkennen.

Colofon



Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Dennis van Kampen (dennis.kampen@minbzk.nl)

Noor Huijboom



TU Delft

Clare Shelley-Egan

María A. Barea





Universiteit van Amsterdam

Joris van Hoboken

Bengi Zeybek



Centre for Quantum and Society (QDNL)

Michiel Schuurman

Meerte van Duuren

Pieter van Kuilenburg

Daniël Frijters



Redactie en vormgeving

Future Communication



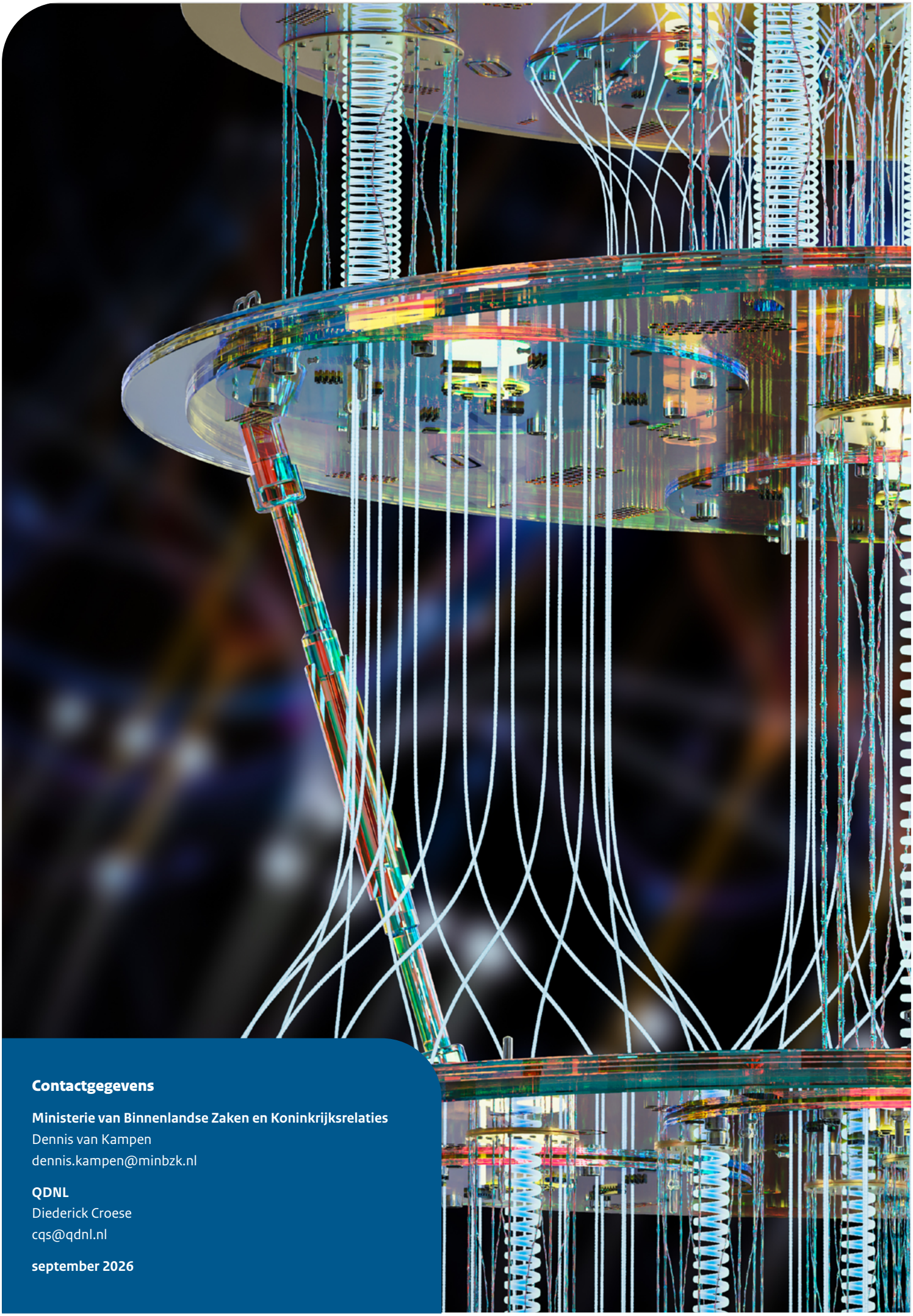
Druk

Xerox



Beeld cover

iStock | PhonlamaiPhoto



Contactgegevens

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Dennis van Kampen
dennis.kampen@minbzk.nl

QDNL
Diederick Croese
cqs@qdnl.nl

september 2026