3
Vragenuur: Vragen Hijink

Aan de orde is **het mondelinge vragenuur**, overeenkomstig artikel 136 van het Reglement van Orde.

Vragen van het lid Hijink aan de minister van Volksgezondheid, Welzijn en Sport over **de handel in privégegevens van miljoenen Nederlanders uit coronasystemen van de GGD**.

De **voorzitter**:
Dan ga ik nu over naar het mondelinge vragenuur. Ik heet natuurlijk iedereen van harte welkom, ook de minister van Volksgezondheid, Welzijn en Sport. Ik geef de heer Hijink namens de SP als eerste vragensteller het woord voor zijn vraag over de handel in privégegevens van miljoenen Nederlanders uit coronasystemen van de GGD. De heer Hijink.

☐

De heer **Hijink** (SP):
Dank, voorzitter. Vandaag, morgen en hopelijk ook de komende tijd, maken tienduizenden, honderdduizenden mensen een afspraak bij de GGD. Bijvoorbeeld als zij een test willen laten doen, of als zij zich laten vaccineren. Sinds gisteren weten we dat dat risico's met zich meebrengt. Sinds gisteren weten we dat op grote schaal de persoonsgegevens die mensen achterlaten bij de GGD door criminelen worden doorverkocht. De SP vindt dat een hele heftige en ernstige zaak. Berichten die rondgaan op het internet zien er ongeveer zo uit: koop je gegevens, koop die data. Er staat zelfs bij: "Wil je iets weten over een persoon? Wij kunnen ook zoeken op een specifieke persoon." Dat wil zeggen dat criminelen inmiddels in het bezit zijn van de gegevens van vele miljoenen Nederlanders. Dan gaat het om woonplaats, adres en mailadres, maar ook het bsn-nummer en het telefoonnummer. Met die data kun je hele nare dingen doen. Daar kun je crimineel gedrag mee laten zien. Daar kun je mensen mee afpersen. Daar kun je phishingmails mee versturen aan mensen. Daar kun je de meest gruwelijke dingen mee doen en mensen mee in de vernieling helpen. Wij tillen daar heel zwaar aan en daarom zou ik de minister willen vragen: wat gaat hij doen om de testbereidheid in ons land overeind te houden en om ervoor te zorgen dat mensen nog steeds een test laten doen, in de wetenschap dat hun gegevens wel veilig zijn? Wat gaat hij doen om de gegevens van mensen nu veilig te stellen? Niet over een maand, niet over een halfjaar, maar nu?

De **voorzitter**:
Dan geef ik nu het woord aan de minister.

☐

Minister **De Jonge**:
Voorzitter, dank. Ik deel zeer met de heer Hijink dat het hier gaat over een hele ernstige zaak. Daarom allereerst hulde voor Daniël Verlaan, een journalist van RTL, die afgelopen vrijdag melding maakte bij de GGD, zodat de GGD aangifte kon doen, zodat de politie onderzoek kon doen en zodat er inmiddels twee aanhoudingen zijn verricht die verband houden met deze zaak. Het is een hele ernstige zaak. Als je een beroep doet op de GGD, moet je weten dat je gegevens veilig zijn. Daarom moet het informatiebeheer bij de GGD gewoon aan de hoogste standaarden voldoen ten aanzien van de veiligheid, zowel voor van buiten naar binnen kunnen komen in de GGD-systemen, maar ook voor het mogelijkerwijs verspreiden van binnen naar buiten. Er werken heel veel mensen bij de GGD en daarom is het zo dat alle GGD'en uiteraard voor alle mensen die ze aannemen ervoor zorgen dat ze een opleiding genieten, dat ze in het bezit zijn van een geldige vog en dat ze geheimhoudingsverklaringen ondertekenen. Implicaties van de vertrouwelijkheid van het werk zijn continu onderwerp van training en gesprekken. Sinds de start van de pandemie controleert de GGD uiteraard continu het gebruik van de systemen. In december hebben we samen met de GGD een risicoanalyse laten uitvoeren en zijn er maatregelen getroffen om de beveiliging te verhogen. Zo voldoet het systeem inmiddels aan de laatste norm voor informatiebeveiliging in de zorg, de NEN 7510. De mensen die werken bij de GGD hebben alleen toegang tot persoonsgegevens wanneer dit noodzakelijk is. Bij verboden toegang volgt ontslag en als het nodig is aangifte bij de politie.

Na deze tip zijn er extra maatregelen getroffen om de pakkans te vergroten. Er worden nog meer controles uitgevoerd en die controles worden ook geautomatiseerd, zodat ze volcontinu kunnen worden uitgevoerd, om daarmee te pakkans te vergroten voor mensen die in de vorm van een samenzwering van plan zijn om die gegevens te verkopen aan partijen die daar verder kwaads mee in de zin hebben. Uiteraard hebben we de GGD hulp aangeboden en uiteraard ondersteunen we de GGD waar we kunnen. De GGD zet alles in het werk om de vanaf december getroffen maatregelen naar aanleiding van wat er vrijdag gebeurd is, nog verder te versnellen. De GGD heeft ook aanleiding gezien om een externe partij te vragen om te controleren of het gat nu echt gedicht is en of het nu echt niet meer mogelijk is om de beveiliging verder op te voeren. Die externe partij is ook om een audit gevraagd. De uitkomsten daarvan deel ik uiteraard met de GGD.

De heer **Hijink** (SP):
Ik hoor eigenlijk de minister op geen enkele manier de garantie uitspreken dat de gegevens die mensen nu achterlaten bij de GGD ook daadwerkelijk veilig zijn. Er komt een audit, er komt een onderzoek, er komen misschien aanvullende maatregelen, maar ik hoor de minister niet zeggen: wij hebben dit probleem nu dusdanig goed in beeld dat we het ook kunnen oplossen. Dat hoor ik hem niet zeggen. Ik vind dat schokkend. Wij hebben hier voor de zomer vorig jaar een brief gekregen van de minister, waarin hij schreef: CoronIT — dat is het systeem dat toen gebruikt werd — voldoet aan alle eisen aan het veilig gebruik van gegevens van burgers. We hebben in september een uitzending van Nieuwsuur gehad waarin al werd blootgelegd dat honderden medewerkers van de GGD in alle bestanden konden meekijken, in alle bestanden van alle Nederlanders, dat je daarin gericht kon zoeken op specifieke personen om hun gegevens, ook medische gegevens, te achterhalen. Dit speelt dus al maanden! Het probleem is dus niet: we gaan nu een audit doen. Nee, het probleem is hoe er ooit een systeem gebouwd heeft kunnen worden waardoor honderden, duizenden mensen toegang hebben tot alle gegevens. Het hoort in geen enkel ICT-systeem zo geregeld te zijn dat zo veel mensen bij zo veel data kunnen. Dat is al een gevaar op zich. Ik wil van de minister ook weten op welk moment hij bij de GGD aan de bel heeft getrokken en gezegd: ho,

wat hier gebeurt, is niet goed. Waarom heeft hij dat in september bijvoorbeeld niet meteen al gedaan, toen Nieuwsuur dat zo naar buiten bracht? Dat was het moment geweest voor deze minister om te zeggen: dit kunnen wij niet accepteren, hier grijpen wij op in.

Minister **De Jonge**:
De GGD heeft uiteraard alles gedaan wat nodig en mogelijk is om de systemen verder te beveiligen. Naar aanleiding van de audit en de onderzoeken die zijn gedaan aan het einde van vorig jaar, zijn verdere beveiligingsmaatregelen getroffen. Ik hecht eraan een aantal dingen te onderstrepen. Eén is dat ik het zeer eens ben met de heer Hijink dat alles moet worden gedaan om die systemen zo veilig mogelijk te maken, want het vertrouwen in hoe de GGD met gegevens omgaat, helpt de testbereidheid. Daarover geen misverstand. Maar dan heel precies over wat hier nu is gebeurd. Het gaat hier waarschijnlijk over mensen die doelbewust een criminele daad hebben gepleegd, dus doelbewust gegevens hebben gekopieerd die in het systeem aanwezig zijn en daarmee handel hebben gedreven. Dat is wat hier aan de orde is. Het gaat niet zozeer over de systeembeveiliging as such, als wel om gedragingen die hebben geleid tot iets wat je gewoon een criminele daad, een misdrijf zou kunnen noemen.

Twee. CoronIT voldoet natuurlijk wel degelijk aan de laatste standaarden als het gaat over de informatiebeveiliging en wat die systemen betreft is het wel degelijk zo dat je met name díé gegevens in kunt zien, die je ook nodig hebt voor je werk. Als je een afspraak moet maken voor een test — want daar gaat CoronIT over — dan moet je naam en adresgegevens hebben. Als je een uitslag moet doorbellen, moet je de uitslag kunnen inzien, anders kun je hem niet doorbellen. Als je een afspraak moet maken over vaccins, moet je over medische gegevens kunnen praten, want je moet weten wat de contra-indicaties zijn en of iemands medische toestand in combinatie met die contra-indicaties betekent dat je de afspraak voor vaccinatie nu niet moet maken.

Kortom, sommige gegevens heb je als medewerker bij de GGD nou juist nodig. Dan kan het dus niet anders dan dat je het zo inregelt dat de medewerkers bij die gegevens kunnen, maar alleen bij die gegevens die ze nodig hebben voor hun werk — daar ben ik het zeer mee eens — en daarnaast met alle vertrouwelijkheid die je mag verwachten van mensen die met persoonsgegevens omgaan. Daarvoor wordt aan de voorkant gescreend door middel van een vog. Er wordt in de opleiding aandacht aan besteed. Mensen worden eruit gegooid op het moment dat blijkt dat ze zich niet conform de vertrouwelijkheid hebben gedragen. Mensen moeten een geheimhoudingsverklaring ondertekenen. De pakkans bij misbruik van gegevens wordt verhoogd door de periodieke controles zo vaak mogelijk te laten plaatsvinden en volautomatisch te laten draaien. Kortom, alles wordt gedaan om te zorgen dat het zo veilig mogelijk is, maar uiteindelijk is tegen dit type misdaad natuurlijk geen kruid gewassen.

De heer **Hijink** (SP):
Het is ontzettend jammer dat de minister zo afsluit, want "geen kruid tegen gewassen"? Een overheid zou er alles aan moeten doen om dit soort misdaden te voorkomen. Die moet haar systemen dusdanig inregelen en beveiligen dat niet één iemand die kwaadwillend is, de hele computer kan leegtrekken, alle data naar zich kan toetrekken, op Marktplaats kan zetten en zijn zakken kan vullen. Dat hoort een goede overheid natuurlijk te voorkomen. Er zullen altijd mensen zijn die misbruik maken van de data die in een systeem beschikbaar zijn. Er zullen altijd mensen zijn die op zoek gaan naar manieren om crimineel gedrag te laten zien. Het is juist aan de overheid om dat te voorkomen, en dat kun je wel degelijk doen als je op tijd had gezorgd dat de privacy in dat systeem op orde was geweest en dat niet tienduizenden mensen bij de GGD inzage hebben in honderdduizenden dossiers van mensen. Dat had natuurlijk voorkomen moeten worden. Erkent de minister dat dan ook? Hij zegt nu: we doen audits en de pakkans wordt verhoogd. De enige reden dat wij hier nu staan, is omdat een journalist van RTL, Daniël Verlaan, slim genoeg is geweest om te achterhalen dat deze data al wijdverspreid op internet verkocht worden. Dat is de enige reden dat wij hier staan, niet omdat deze minister en deze overheid de systemen zo goed op orde hebben.

Minister **De Jonge**:
Hulde voor Daniël Verlaan, en zeker ook voor de melding die hij heeft gedaan. Daardoor kon de GGD aangifte doen, waardoor inmiddels een aantal mensen zijn aangehouden die hierbij betrokken zijn geweest. Het strafrechtelijk onderzoek loopt. Ik denk dat dat sowieso goed is. Daarnaast is het natuurlijk nodig om alles te doen wat mogelijk is om een systeem te beveiligen. Ik heb me zojuist misschien ongelukkig uitgedrukt, maar wat ik bedoel te zeggen is dat het uiteindelijk gewoon een misdrijf is als er echt sprake is van doelbewust de regels overtreden, doelbewust alle beveiligingsmogelijkheden omzeilen voor persoonlijk financieel gewin. Het valt niet mee om alles daartegen te beveiligen, maar ik denk dat je op dat punt alles moet doen wat redelijkerwijs mogelijk is om systemen te beveiligen, om mensen goed te toetsen en te screenen aan de voorkant en continu te screenen tijdens het werk, door autorisaties zo in te richten dat je alleen bij die gegevens kunt waarmee je te maken hebt in je werk. Daar zijn maatregelen voor getroffen. Een extern onderzoek moet helpen om het lek te dichten als er nog een lek is. We zitten uiteraard continu met de GGD om tafel om te kijken wat er anders en beter kan.

De **voorzitter**:
Dan heb ik hier mevrouw Agema, de heer Veldman, mevrouw Buitenweg, mevrouw Van Esch, mevrouw Van den Berg, mevrouw Bergkamp en de heer Van Otterloo. Ik zie ook mevrouw Kuiken. Voor een aanvullende vraag hebben we een halve minuut afgesproken, dus ik hoop dat iedereen zich daaraan houdt, anders moet ik jullie midden in jullie zin afbreken en dat is niet ook niet altijd fijn. Dan ga ik eerst naar mevrouw Agema namens de PVV.

Mevrouw **Agema** (PVV):
Het is stuitend dat de minister hier zegt dat hij er eigenlijk niks aan kan doen dat gegevens gestolen kunnen worden wanneer een crimineel inbreekt op een systeem. Het is stuitend. Deze minister is verantwoordelijk voor dit systeem. Als het gaat om het verhogen van de pakkans, dan is het gewoon een slap verhaal. De minister moet hier eens uit-

leggen waarom hij voor het afnemen van een test de adresgegevens van mensen nodig heeft.

Minister **De Jonge**:
Persoonsgegevens zijn natuurlijk nodig om de uitslag te kunnen communiceren en zijn ook nodig omdat je als persoon moet kunnen inloggen. Je wilt nou juist persoonsgegevens om te voorkomen dat een testuitslag vervolgens bij de verkeerde terechtkomt.

Mevrouw **Agema** (PVV):
Maar de GGD komt toch niet bij de mensen thuis de test afnemen? Je moet toch naar de teststraat toe? Waarom vraagt de minister privé-informatie van mensen — denk aan adresgegevens en dit soort gevoelige gegevens — terwijl de GGD helemaal niet bij de mensen thuis een test komt afnemen? Het is overbodige informatie voor een overheid die te gewillig is op het opeten van informatie van mensen. Mensen worden nu het slachtoffer van identiteitsfraude door deze minister, die verantwoordelijk is voor een systeem dat door en door lek is. Criminelen kunnen hun gang gaan en de minister heeft geen beter verhaal dan dat hij de pakkans wil verhogen. Hij moet nu overgaan op een systeem dat uitsluitend het hoognodige van mensen vraagt en dat niet vraagt om de hele janboel, alle medische gegevens, adresgegevens en alle gegevens waar de GGD niets mee te maken heeft voor een afnemen van een test.

Minister **De Jonge**:
Ik geloof niet dat deze weergave van de werkelijkheid klopt. Er worden wel degelijk hoge eisen gesteld aan de systeembeveiliging waarmee wordt gewerkt. Dat heb ik zojuist toegelicht. Om risico's te dichten is er een risicoanalyse uitgevoerd. Naar aanleiding daarvan zijn verbetermaatregelen getroffen die versneld worden geïmplementeerd naar aanleiding van wat zich heeft voorgedaan. Daarnaast wordt extern geaudit of het gat daarmee daadwerkelijk gedicht is, want dat willen we natuurlijk. Dat is één. Twee. Het gebruik van persoonsgegevens is juist bedoeld om te voorkomen dat je vervolgens een testuitslag doorbelt naar iemand bij wie de test helemaal niet is afgenomen. Je hebt dus juist DigiD, naw-gegevens en bsn-gegevens nodig om te weten met wie je te maken hebt. Dat is volmaakt logisch. Dat gebeurt trouwens echt overal in de zorg en overal in het contact tussen overheid en burger. Dat is nou juist om ervoor te zorgen dat je medische gegevens koppelt aan de juiste persoon en je daarmee geen vergissing begaat.

De heer **Veldman** (VVD):
Dit lek lijkt toch wel iets ernstiger dan de minister in zijn antwoord voorstelt. Het gaat namelijk niet om een enkele medewerker die wat heeft lopen grasduinen in systemen; het gaat om grootschalige handel van allerlei persoonsgegevens van allerlei mensen die zich hebben laten testen. Mijn vraag is als volgt. Rondom het vaccineren werken we niet alleen met de GGD, maar ook met de huisartsen en de ziekenhuizen. De minister heeft steeds gezegd: de vertraagde start van het vaccineren in Nederland, dat als laatste in Europa begon, komt ook door de ICT-systemen; we moeten het namelijk zorgvuldig doen en we moeten die systemen op orde hebben. Kan de minister garanderen dat de systemen die nu gebruikt worden voor het vaccineren op orde zijn, dat we niet tegen eenzelfde soort fraude aan lopen en dat we niet tegen eenzelfde soort grootschalige illegale uitwisseling van gegevens aan lopen?

Minister **De Jonge**:
Er moeten twee dingen uit elkaar gehaald worden. Ik ben het zeer eens met de heer Veldman dat hier sprake is van fraude en handel in wedderrechtelijk verkregen informatie, absoluut. Het is gewoon een criminele daad. Er is aangifte gedaan, er loopt een strafrechtelijk onderzoek, mensen zijn aangehouden et cetera. Dat is één. Twee. De systemen moeten zo goed mogelijk beveiligd kunnen worden om de kans daarop zo klein mogelijk te maken. Daarom moeten maatregelen genomen worden om de pakkans te vergroten. Er moet sowieso aan de voorkant voor gezorgd worden dat mensen die kwaad in de zin hebben niet binnen kunnen komen. Wat zeker speelt, is dat je dezelfde hoge eisen moet verbinden aan alle systemen die worden gebruikt. U weet dat we verschillende uitvoerders hebben van de vaccinatie, onder andere de GGD. Alle uitvoerders — dat geldt dus voor de huisartsen en ook voor alle andere prikkende partijen — gebruiken hun eigen systemen, met de beveiliging die daarbij past. Denk aan de epd's voor de verpleeghuizen. De huisartsen gebruiken hun eigen HIS'en. De GGD gebruikt het systeem van de GGD. Daarvoor is uiteraard afgebakend dat alleen de mensen die iets moeten doen met een vaccinatie in het vaccinatiedeel van de systemen kunnen kijken. De mensen die bijvoorbeeld testafspraken maken, kunnen niet kijken in het vaccinatiedeel. De mensen die alleen met vaccinaties bezig zijn, kunnen dat wel. Dat heeft gewoon te maken met autorisatie.

De **voorzitter**:
Meneer Veldman, uw tweede, aanvullende, vraag.

De heer **Veldman** (VVD):
Dat klinkt mooi en eenvoudig, maar de werkelijkheid is meestal anders. Bij het vaccineren hebben we ook nog te maken met het feit dat de systemen met elkaar geïntegreerd moeten worden. Althans, dat was de uitleg van de minister over de vertraagde start. Het was niet alleen het systeem van de GGD; ook de huisartsen hebben hun systeem en ook ziekenhuizen hebben hun systeem. Het moest naar één systeem geïntegreerd worden. Er wil nog weleens wat misgaan als systemen met elkaar moeten samenwerken of integreren. Welke garanties geeft deze minister dat dit niet fout gaat?

Minister **De Jonge**:
Er is hier geen kwestie van het integreren van systemen. Wat toen nodig was — dan spreken we van de periode van december — was dat de aanpassing van het systeem van de GGD, van CoronIT, nog moest worden afgerond. Daar was toen sprake van. Er is natuurlijk een koppeling met het centrale registratiesysteem van het RIVM, maar hier speelt geen kwestie van integratie van systemen. Hier speelt wel dat voor CoronIT, als een van de systemen die door de GGD wordt gebruikt, überhaupt geldt dat het aan de hoogste standaarden moet voldoen. Dus moeten we al de maatregelen die op basis van de audit in december in gang zijn gezet versneld uitvoeren. Dat is wat de GGD heeft laten weten. De GGD vraagt daarnaast extern onderzoek om te

toetsen of de gaten daarmee echt gedicht zijn. Dat geldt dus voor het systeem CoronIT, waar zowel de vaccinaties op draaien als het testen.

De **voorzitter**:
Mevrouw Buitenweg, namens GroenLinks, en dan mevrouw Van Esch.

Mevrouw **Buitenweg** (GroenLinks):
De minister heeft het veel over dat de systemen veilig moeten zijn en gecontroleerd moeten worden. Maar wat hier volgens mij het belangrijkste is, is privacy by design. De minister kent dat goed, want daar hebben we het bij de corona-app ook veelvuldig over gehad. Ik denk dat de vraag is — daar had mevrouw Agema natuurlijk wel een punt — hoe het systeem nou in elkaar zit en of echt alleen de gegevens worden gevraagd die noodzakelijk zijn. Wat voor eisen zijn er gesteld aan privacy by design aan de GGD en volgt de GGD al die eisen ook op? Hoeveel mensen hebben dan als gevolg daarvan binnen de GGD echt toegang tot die gegevens? Hoeveel mensen, hoeveel personen, hebben potentieel toegang tot mijn gegevens als ik zo meteen naar de teststraat loop?

Minister **De Jonge**:
Ik ben het zeer met mevrouw Buitenweg eens. Dat is inderdaad zoals het zou moeten. Het design moet zo zijn dat alleen de gegevens kunnen worden opgevraagd die daadwerkelijk noodzakelijk zijn. Mevrouw Agema vraagt: waarom eigenlijk het bsn? Dat is omdat het hier gaat over een medisch dossier. Dan is het bsn verplicht, want je moet weten dat het medisch dossier gekoppeld is aan de persoon die je daadwerkelijk voor je neus hebt staan. Dat moet je kunnen toetsen. Dus dat is van belang. Voor het overige geldt inderdaad dat je moet willen dat personen alleen toegang hebben tot dat deel van het systeem dat daadwerkelijk belangrijk is voor het werk dat ze doen. Even naar de GGD vertaald: iemand die testafspraken maakt, hoeft niet je vaccinatiedossier in te zien. Dat is niet nodig. Dat moet dus van elkaar gescheiden worden. Dat is met een functiescheiding gescheiden. Wat in de systemen bij de GGD gebeurt, is dat alle checks-and-balances de komende tijd opnieuw tegen het licht worden gehouden om te bekijken of ze daadwerkelijk aan de hoogste standaarden voldoen.

Mevrouw **Buitenweg** (GroenLinks):
Ten eerste was het iets anders wat mevrouw Agema zei, maar ik laat haar eigen zaken bij haar. Het ging over het adres, dat niet noodzakelijk zou zijn. Mijn vraag is nog een andere. De minister zegt: eigenlijk moeten alleen die mensen toegang hebben tot de gegevens voor wie dat nodig is. Ja, dat is een algemeenheid. Daar ben ik het helemaal mee eens. De vraag is of er echt heel duidelijke eisen zijn gesteld aan wie er dan inderdaad toegang toe moet hebben. Ik stelde ook een concrete vraag: als ik nu zo meteen naar de teststraat loop, hoeveel mensen van de GGD hebben dan in de komende maanden potentieel toegang tot mijn gegevens? Want daar gaat natuurlijk over. Het gaat niet over wat het principe van privacy by design in zijn algemeenheid is. Dat weten we allebei. Maar hoe heeft de minister dat nou handen en voeten gegeven en waar leidt dat toe? Hoeveel mensen hebben dan dus toegang tot mijn gegevens?

De **voorzitter**:
Ja, concrete vraag.

Minister **De Jonge**:
De GGD heeft voor dat deel dat gaat over de testafspraken die mensen gemachtigd die die testafspraken moeten maken. Het deel van de mensen dat bron- en contactonderzoek doet — dat is weer een ander systeem, overigens — heeft toegang tot het systeem dat het bron- en contactonderzoek ondersteunt. De mensen die betrokken zijn bij vaccinatie, hebben toegang tot het systeem voor vaccinatie. Zo hoort het geregeld te zijn. Met die functiescheiding is het ingeregeld bij de GGD.

De **voorzitter**:
Nee, mevrouw Buitenweg.

Mevrouw **Buitenweg** (GroenLinks):
Voorzitter, ik heb geen antwoord gekregen. Ik heb twee keer dezelfde vraag gesteld.

De **voorzitter**:
Klopt.

Mevrouw **Buitenweg** (GroenLinks):
Gaat het over honderden mensen, duizenden mensen of tien mensen?

Minister **De Jonge**:
De bron- en contactonderzoekers zijn 8.000 fte's, dus dat zijn er nogal wat.

De **voorzitter**:
Dus 8.000 mensen hebben toegang?

Minister **De Jonge**:
Als het gaat over bron- en contactonderzoek wel. De testafspraken zijn er een paar duizend, via een callcenter. Zo werkt het, jongens.

De **voorzitter**:
Dan mevrouw Van Esch. Als ik u de gelegenheid geef, mevrouw Buitenweg, moet ik iedereen de gelegenheid geven om een derde aanvullende vraag te stellen en dat is niet de bedoeling, vandaar.

Mevrouw **Van Esch** (PvdD):
Ik vind dat aantal van 8.000 toch wel heftig om te horen. Toch wel fijn dus om die informatie nog te hebben.

Ik wil nog een vraag stellen over een ander systeem waarin volgens mij precies dezelfde cruciale privacyissues zouden kunnen ontstaan, namelijk dat opt-insysteem. Er zijn op dit moment 8 miljoen medische dossiers opengesteld; nog steeds, ondanks dat we al herhaaldelijk hebben gevraagd wanneer dat nou weer gaat sluiten. En ook hierbij kunnen mensen onbevoegd toegang hebben tot medische dossiers van mensen. Ik vind dat een zeer zorgwekkende zaak. Precies hier kan hetzelfde gebeuren als we nu hebben gezien bij dit coronasysteem. Dus wanneer zetten we nou alsjeblieft dat opt-insysteem uit? Ik zeg er "alsjeblieft" bij, voorzitter, want dit is echt een heel groot risico en hetzelfde risico als waar we nu over spreken. Ik vraag me dus af waarom we dat nog steeds openstellen; dat kan écht niet.

Minister **De Jonge**:
Ik denk dat mevrouw Van Esch hier bedoelt het opt-insysteem voor gegevensdeling tussen huisartsen. Dat is bedoeld om enorme wachtlijsten te voorkomen. Ik denk dat mevrouw Van Esch dat bedoelt.

De **voorzitter**:
Misschien kunt u dat even kort toelichten, mevrouw Van Esch.

Mevrouw **Van Esch** (PvdD):
Ik doel op het opt-insysteem voor medische gegevens. Normaal moet je er toestemming voor geven voordat jouw gegevens überhaupt kunnen worden gedeeld. Op dit moment zijn die gegevens van 8 miljoen Nederlanders gewoon opengesteld. Dus de medische gegevens van deze mensen kunnen inderdaad worden gedeeld. In het begin van de coronacrisis kon daar nog enigszins een logica in zitten ...

De **voorzitter**:
U zou alleen een toelichting geven.

Mevrouw **Van Esch** (PvdD):
... maar dit kan echt niet meer, want we zien welke grote risico's daaraan verbonden zijn. Het is precies hetzelfde risico als we nu ook zien bij de kwestie die we nu bespreken.

Minister **De Jonge**:
Dit is echt een hele andere zaak, maar ik ga mevrouw Van Esch toezeggen dat ik hier schriftelijk op terugkom. Dit is echt een heel andere zaak. Ik ben er op dit moment niet tot op de laatste stand van zaken op voorbereid, maar dit gaat over het kunnen delen van medische gegevens, om een enorme opstopping in de keten te voorkomen. Dat is waar het hier om gaat. Ik zeg u toe om u de laatste stand van zaken op dat punt te laten weten.

De **voorzitter**:
Een tweede, aanvullende vraag, mevrouw Van Esch.

Mevrouw **Van Esch** (PvdD):
Het gaat hier om dezelfde methode.

Ik wil toch nog een tweede vraag stellen. Die gaat nog steeds over die zogenoemde "exportfunctie". Die is nu stilletjes een beetje weggemoffeld uit het systeem, maar volgens mij was dat echt een van de tekortkomingen. Je moet je toch rotschrikken als er zo'n exportfunctie in zit? Daarmee kun je miljoenen dossiers zo hup, met één druk op de knop downloaden. Gaat de minister nu bijvoorbeeld een team van ethische hackers inzetten om al die systemen, al die medische systemen die we in Nederland hebben, op z'n minst op zo'n exportfunctie te laten controleren? Want het kan toch niet zo zijn dat dit soort functies zitten in Nederlandse medische systemen waar de overheid verantwoordelijk voor is?

Minister **De Jonge**:
Iedere instelling is verantwoordelijk voor haar eigen omgang met data. En als er sprake is van een datalek, is iedere instelling ook verplicht om dat te melden aan de Autoriteit Persoonsgegevens, op grond van de AVG. En dat gebeurt ook. Mevrouw Van Esch heeft het over systemen die onvoldoende veilig zijn. Er worden inderdaad pentesten gedaan, maar er zijn natuurlijk duizenden instellingen met duizenden systemen, dus dat is niet een actie die je vanuit het departement kunt ondernemen. Wat doen we wél vanuit het departement? Er zijn tal van acties waarbij we helpen en ondersteunen bij de informatiebeveiliging en informatieveiligheid. Soms doen we dat gewoon door regels te maken, door wet- en regelgeving. Soms doen we dat door geld te geven, door gewoon een financiële ondersteuning om dingen mogelijk te maken. En heel vaak ook door gewoon praktische ondersteuning. Daarbij helpen we partijen en instellingen om goed om te gaan met hun dataveiligheid. En daar horen ook pentesten bij, testen om te kijken of je van buiten binnen kunt komen in een systeem. Dat deel ik zeker met mevrouw Van Esch.

De **voorzitter**:
Eerst is mevrouw Van den Berg en dan mevrouw Bergkamp. Mevrouw Van den Berg spreekt namens het CDA.

Mevrouw **Van den Berg** (CDA):
Dank u wel, voorzitter. Ook de gegevens van militairen die uitgezonden worden, zitten bij de gelekte gegevens. Dat is volgens het CDA extra ernstig, want deze militairen zijn ook nog eens extra kwetsbaar omdat ze in het buitenland zitten. Maar ik zie een patroon. We staan hier nu voor de vierde keer binnen een jaar. Vorig jaar maart was er een lek bij het RIVM. In juli spraken we over twee schijven die waren vertrokken uit de kluis van het Donorregister. In september hadden we hier een gesprek over wie er allemaal toegang heeft tot gegevens. En nu is er dit weer. Wat gaat de minister er structureel aan doen om dit op te pakken, ook al omdat de Algemene Rekenkamer in het jaarverslag aangaf dat het ICT-beleid sowieso een onvolkomenheid is?

Minister **De Jonge**:
De voorbeelden die u noemt — ik zou er nog meer kunnen noemen — zijn volgens mij voorbeelden van überhaupt onveilige omgang met informatie. U ziet een patroon? Ja, dat patroon is dat informatiebeveiliging de hoogste prioriteit moet hebben, en dat het alle aandacht vraagt om ervoor te zorgen dat het daadwerkelijk veilig is. En waar het misgaat,

moet alles eraan worden gedaan om ervoor te zorgen dat er gaten worden gedicht en dat het lek wordt dichtgestopt. Dat is precies wat er gebeurt. En wat gebeurt er daarnaast in structurele zin? Zowel via wet- en regelgeving, als via ondersteuning en financiële ondersteuning wordt er van alles gedaan om te zorgen dat juist de informatiebeveiliging op orde komt. In al deze gevallen is heel intensief actie ondernomen om de informatiebeveiliging te verbeteren.

Mevrouw **Bergkamp** (D66):
Het is een blamage en het is de volgende blamage. Mijn collega van het CDA gaf het net aan. Het lijkt erop alsof de minister de schuld geeft aan de criminelen, terwijl, als je kijkt naar wat er gebeurt is, dan is dat natuurlijk het falen van het systeem. Mensen hebben toegang tot gegevens die ze niet direct nodig hebben. Mijn vraag aan de minister is de volgende. Hoe worden mensen die slachtoffer zijn geworden van deze datahandel — ik maak me daar zorgen over, over de veiligheid — erover geïnformeerd dat hun gegevens zijn gestolen, zijn doorverkocht? Stel dat je wordt gestalkt. Ik kan me dan voorstellen dat je je niet veilig voelt.

Minister **De Jonge**:
Toch eerst even een reactie op mevrouw Bergkamp. Ja, voor diefstal geef ik inderdaad de schuld aan de mensen die verantwoordelijk zijn voor die diefstal. Dat zijn toch echt de mensen die een screenshot hebben zitten maken en dat screenshot hebben verkocht. Dat is namelijk gewoon een wederrechtelijke manier om informatie te verkrijgen om daar vervolgens persoonlijk gewin uit te halen. Dat is gewoon een criminele daad. Dus ja, daar is aangifte van gedaan. Dat rechtvaardigt een strafrechtelijk onderzoek. Er zijn mensen aangehouden. Dus ik ben inderdaad geneigd om de mensen die verantwoordelijk zijn voor diefstal, namelijk de dieven, verantwoordelijk te houden. Het lijkt me dat we dat inderdaad moeten doen. Twee is dat ik me met mevrouw Bergkamp grote zorgen maak over mensen wier gegevens op straat zijn komen te liggen. Wat precies de omvang daarvan is en voor wie dat geldt, is op dit moment niet te zeggen. Dat is onderdeel van zowel het onderzoek van de politie als het forensische onderzoek dat de GGD zelf in eigen huis uitvoert. Dat komt natuurlijk ook bij elkaar: het strafrechtelijk deel en het forensisch deel dat de GGD zelf uitvoert. We zullen op een nader moment moeten bekijken wat de omvang daarvan is, wie het betreft en welk type ondersteuning daar gepast is. Daar moeten we zeker aandacht voor hebben, absoluut.

De **voorzitter**:
Dan zie ik de heer Van Otterloo en dan mevrouw Kuiken. De heer Otterloo, namens 50PLUS.

De heer **Van Otterloo** (50PLUS):
Ik sluit mij aan bij alle vragen over het systeem, maar ik zou ook even naar de eerste fase willen, namelijk: hoe komt het dat deze mensen wel op die plek zijn terechtgekomen? Is het al helder of dat een geplande actie was of meer "gelegenheid maakt de dief"?

Minister **De Jonge**:
Het laatste weet ik niet. Het strafrechtelijk onderzoek loopt. Er zijn twee aanhoudingen verricht. Ik weet ook niet of het daarbij blijft. Het zouden er ook nog meer kunnen worden. Dat weet ik niet. Dat valt op dit moment dus niet te zeggen. Het motief valt echt op dit moment niet te achterhalen. Wat ik wel weet is dat daar waar mensen worden aangenomen om om te gaan met persoonsgegevens, er natuurlijk een goede check aan de voorkant moet zitten. Dat betekent een vog, natuurlijk. Dat betekent het ondertekenen van een geheimhoudingsverklaring. Dat betekent aandacht in de opleiding. Dat betekent vervolgens een lange lijst aan checks-and-balances intern, de controle op systemen om de pakkans te vergroten. Dat is wat er allemaal gebeurt. En dan toch kan dat ook weer niet voorkomen dat iemand die echt kwaad in de zin heeft, tot acties komt die je niet hebt kunnen voorkomen. Wel wil je pakkans zo groot mogelijk laten zijn. Natuurlijk, want dat is wat moet. Maar echt helemaal uitsluiten, helemaal voorkomen, dat is toch wel heel erg lastig.

De heer **Van Otterloo** (50PLUS):
Een tweede vraag. Ik begrijp dat op dit moment nog niet duidelijk is waar het probleem is ontstaan dat deze mensen toegang kregen om vervolgens misbruik te maken van hun bevoegdheden.

Minister **De Jonge**:
Er zitten checks-and-balances aan de voorkant, dus de vog, de scholing, de geheimhoudingsverklaring, al dat soort dingen. De controle op de systemen waarvan men gebruikmaakt, de autorisatie, dus de toegang tot welke databases, dat heb je in de hand. Als werkgever heb je dat in de hand. Als iemand echt kwaad in de zin heeft, screenshots maakt en die wegstuurt bijvoorbeeld, en die verkoopt, dan is daar geen kruid tegen gewassen. Dat is een beetje wat hier speelt.

Mevrouw **Kuiken** (PvdA):
Ik heb toch het idee dat minister De Jonge er iets te makkelijk overheen stapt. Immers, gisteren is nog de exportfunctie eruit gehaald. Moeten we dan niet concluderen dat in ieder geval een aantal belangrijke veiligheidsmaatregelen niet zijn genomen? En ten tweede: gisteravond is er nog data aangeboden voor verhandeling. Dit is al maanden gaande. Blijkbaar was iedereen erbij, maar heeft niemand het gezien. Mijn vraag is dan ook: constateert de minister met mij dat we het simpelweg niet weten omdat er dus geen zicht is op wat er feitelijk onder de neuzen plaatsvond?

Minister **De Jonge**:
Er is juist geconstateerd dat het beveiligingsniveau omhoog kan, dus dat er hogere eisen te stellen zijn aan die veiligheid. Dat is eind vorig jaar geconstateerd. Toen is er een set aan maatregelen genomen. Een aantal van die maatregelen worden versneld doorgevoerd. Een van die maatregelen is inderdaad wat u al noemde: de exportfunctie is geschrapt, niet zozeer uit CoronIT, maar juist uit dat andere programma, HPZone. Dat is een maatregel die nu versneld wordt doorgevoerd. De komende tijd moeten we juist versneld ook al die andere beveiligingsmaatregelen doorvoeren, waarvan in december was geconcludeerd dat dat moet.

Daarbovenop heeft de GGD aan een externe partij gevraagd om nog een keer te toetsen of daarmee dan echt het maximum is gedaan om de dataveiligheid te waarborgen. Want dat is inderdaad wat nodig is.

De **voorzitter**:
Mevrouw Kuiken, tweede vraag.

Mevrouw **Kuiken** (PvdA):
Men wist een aantal maanden geleden al dat het niet veilig genoeg was. Maar pas nu de heer Verlaan, journalist, met deze informatie naar buiten komt, gaat men versneld over tot onder andere het eruit halen van die exportfunctie. Dan is toch echt mijn oprechte vraag: waarom is dat niet eerder gebeurd? Het gaat om bsn-nummers, het gaat om adresgegevens en het gaat over data van mensen die sowieso publiek kwetsbaar zijn. Dan moet je toch meteen alles op alles zetten om dat goed te regelen? Is dat dan niet een teken dat we nog totaal naïef of handelingsverlegen zijn, als het gaat om de privacy en gegevensbescherming van mensen? Dat had toch meteen moeten gebeuren en niet nu pas, nadat er weer een journalist is die aan de bel trekt?

Minister **De Jonge**:
Dat denk ik niet. Overigens ben ik heel blij dat een journalist aan de bel trekt. Op basis daarvan zijn aanvullende maatregelen genomen. Maar we hebben samen met de GGD een risicoanalyse uitgevoerd. Overigens is überhaupt ten aanzien van het hele testsysteem een risicoanalyse uitgevoerd. Er zijn maatregelen getroffen om de beveiliging te verhogen. Het systeem voldoet aan de laatste NEN-norm. Maar u heeft helemaal gelijk. Er was en er is meer mogelijk om die beveiliging verder op te voeren. Al datgene wat mogelijk is om de beveiliging verder op te voeren, moet dus ook worden gedaan. Dat laat onverlet dat uiteindelijk iemand die echt kwaad in de zin heeft daadwerkelijk tot een actie kan komen die je gewoon als een misdrijf moet kwalificeren. Maar in de systemen moet alles worden gedaan om de veiligheid maximaal te waarborgen.

De heer **Hijink** (SP):
Ik vind de nonchalance van de minister echt niet oké. Hoe dit gaat, is echt niet goed. Natuurlijk, bij boeven die met data aan de haal gaan en gegevens stelen, zit het probleem. Die moet je keihard aanpakken, oppakken en straffen. Maar boeven krijgen alleen maar de kans als anderen ook de achterdeur wagenwijd openzetten. Dat is in dit geval gebeurd. Als je een systeem hebt waarvan de minister net zei dat alleen al bij het bron- en contactonderzoek 8.000 mensen toegang hebben tot alle data, dat mensen die het testen moeten inplannen, duizenden mensen, toegang hebben tot de gegevens, de medische data van vele duizenden, tienduizenden, honderdduizenden Nederlanders, dan is er in het ontwerp van het systeem toch iets grandioos mis? Dan kan de minister niet alleen maar zeggen: het zijn de boeven en die moeten in de gevangenis. Nee, de overheid moet zorgen dat we een systeem hebben dat niet zo ontzettend kwetsbaar is. Deelt de minister dat?

Minister **De Jonge**:
Wat ik deel, is dat kwetsbaarheden in het systeem moeten worden aangepakt en dat de maatregelen die daarvoor nodig zijn moeten worden getroffen. Dat iemand die kwaad in de zin heeft uiteindelijk dat kwaad kan uitvoeren, laat onverlet de opdracht aan de overheid, of in dit geval niet de overheid maar de GGD, om alles te doen wat mogelijk is om een systeem maximaal te beveiligen. Ik denk dat daar werk in te doen is. Dat weten we op basis van de risicoanalyse die in december is gedaan. De maatregelen die daarin werden voorgeschreven, worden ook getroffen. Daar waar ze versneld moeten worden getroffen, worden ze versneld getroffen. Daarnaast laat de GGD een externe check uitvoeren om te zien of dit het maximale is wat gedaan kan worden om inderdaad de gaten te dichten. Daarmee bedoel ik ook dat wordt gekeken of bijvoorbeeld de interne toegang van bepaalde personen tot bepaalde gegevens nog verder zou kunnen worden beperkt. Sowieso is het gecompartimenteerd in die zin dat je toegang hebt tot de gegevens waar je wat mee moet, dus dat je bijvoorbeeld toegang hebt tot het adresbestand over de mensen die een testafspraak hebben gemaakt, als je met die testafspraken bezig bent et cetera. Dus die gecompartimenteerde toegang is op dit moment al ingeregeld, maar of die nog verder in te regelen is, is op dit moment onderwerp van de verbeterplannen.

De **voorzitter**:
De heer Öztürk namens DENK en dan de heer Bisschop.

De heer **Öztürk** (DENK):
Als de minister zijn zaken niet goed op orde heeft, kan hij niet constant de schuld aan de boeven geven, want die maken misbruik van de gaten die er zijn. Dit hele verhaal zorgt ervoor dat heel veel mensen PCR-testen en allerlei andere testen wantrouwen. Ziet u dat in de cijfers? En wat gaat u daadwerkelijk doen om deze mensen een en ander te garanderen zodat ze het gevoel hebben dat, als ze hun gegevens aan de overheid toevertrouwen, hun gegevens bij de overheid blijven?

Minister **De Jonge**:
Ik vind het inderdaad heel belangrijk om te zeggen dat je je gewoon veilig kunt laten testen. Er wordt namelijk het maximale gedaan om toe te zien op de informatieveiligheid. Als iemand kwaad in de zin heeft en een criminele daad begaat, dan wordt er aangifte gedaan en dan worden die mensen opgepakt. Zo hoort het ook te lopen. Ik denk dat we ervoor moeten oppassen om boeven te legitimeren door te zeggen: als boeven een kans hebben, gaan ze die kans natuurlijk pakken. Ik denk dat je van instellingen of overheidsorganisaties, in dit geval van de GGD, mag verwachten dat als er mensen worden aangenomen, er aan de voorkant goed wordt gescreend wie er wordt aangenomen en dat er vervolgens alles aan wordt gedaan om te zorgen dat de informatie veilig is. Ik heb u zojuist beschreven welke stappen daarvoor worden gezet. Wat doe je daarmee? Daarmee dien je de testbereidheid van mensen en het vertrouwen dat mensen mogen hebben in de GGD.

De heer **Öztürk** (DENK):
Maar blijkbaar lukte dat niet in de afgelopen maanden. Het zijn heel vaak journalisten die ons informeren dat het niet

lukt. Wanneer denkt u dat iedereen daar echt met een goed gevoel heen kan gaan? Of heeft u een ander systeem, waarbij burgers misschien wat minder privacyinformatie hoeven te geven maar waarbij ze alsnog een PCR-test kunnen laten doen? Mensen krijgen op dit moment het gevoel: het lukt hen niet; mijn gegevens kunnen op straat terechtkomen. Kunt u een ander systeem bedenken of is er een ander systeem waarbij de burger met minder gegevens toch een PCR-test kan laten doen?

Minister **De Jonge**:
Nee. Wat we moeten doen, is het systeem maximaal beveiligen — daar wordt van alles aan gedaan — opdat mensen gewoon vertrouwen hebben in het systeem dat wordt gebruikt.

De heer **Bisschop** (SGP):
Het gaat over systemen die falen en over boeven. Dat is terecht, maar ik wil het over de mensen hebben, over de slachtoffers. Als ik getest ben, hoe weet ik dan of mijn gegevens buiten het systeem bekend zijn geworden en deel uitmaken van criminele activiteiten? En wat breder getrokken: hoe worden de slachtoffers geïnformeerd dat zij hiervan het slachtoffer zijn geworden?

Minister **De Jonge**:
Dit was ook de vraag van mevrouw Bergkamp. Ik heb gezegd dat we dat op dit moment nog niet precies weten. Dat is namelijk onderwerp van strafrechtelijk onderzoek. Wat is de reikwijdte van het misbruik dat hier gepleegd is? Dat weten we eerlijk gezegd op dit moment nog niet. Daarvoor moeten we het strafrechtelijk onderzoek afwachten. Ik ben het zeer met de heer Bisschop eens dat we aan degenen die hiervan het slachtoffer zijn geweest, bijvoorbeeld omdat hun gegevens op straat zijn komen te liggen of omdat hun gegevens verkocht zijn, zo goed mogelijk tegemoet moeten komen zodra we weten wat de reikwijdte is van het misdrijf dat hier heeft plaatsgevonden. Maar dat kan ik op dit moment gewoon nog niet zeggen.

De heer **Bisschop** (SGP):
Ik wilde eigenlijk mijn tweede vraag voor het laatste onderwerp bewaren, maar ik vind dit toch een heel wezenlijk punt. Hoe ver de reikwijdte gaat ... Het is na te gaan welke mensen slachtoffer zijn geworden van deze criminele activiteiten. De slachtoffers moeten geïnformeerd worden dat zij hiervan slachtoffer zijn geworden. Daar hoef je geen strafrechtelijk onderzoek of wat dan ook voor af te wachten. Hun gegevens zijn buiten het systeem terechtgekomen. Daar wordt mee gehandeld, geld aan verdiend enzovoorts. Dit kan hun privacy schenden en zelfs tot identiteitsfraude leiden. Die mensen moeten toch per ommegaande geïnformeerd worden, bijvoorbeeld door een noodactie? Zet iedereen en alles erop om die mensen te beveiligen.

Minister **De Jonge**:
Ja, maar dan moeten we eerst weten om welke gegevens het gaat en van wie. Daar is echt dat strafrechtelijk onderzoek voor nodig. Dat is juist op dit moment onderdeel van het strafrechtelijk onderzoek. De reikwijdte van de mate waarin gegevens op straat zijn komen te liggen is op dit moment gewoon nog onderwerp van onderzoek, dus dat weten we nog niet. Maar ik ben het zeer met u eens: als gegevens daadwerkelijk op straat zijn komen te liggen, dan moet er natuurlijk alles aan worden gedaan om de slachtoffers daar op z'n minst over te informeren en om te kennen te geven wat zij kunnen doen als hun informatie op straat is komen te liggen. Absoluut.

De **voorzitter**:
Als dat strafrechtelijk onderzoek is afgerond, wordt de Kamer daar dan ook over geïnformeerd?

Minister **De Jonge**:
Uiteraard.

De **voorzitter**:
Want ik voel dat er heel veel vragen zijn blijven hangen en onbeantwoord zijn gebleven. Ik begrijp dat dat niet meteen kan, maar misschien kan dat wel binnen een bepaalde termijn.

Minister **De Jonge**:
Dat is altijd aan het Openbaar Ministerie, dus die termijn ken ik niet. Maar ik zet uiteraard wel met de GGD de stappen die nodig zijn om de informatiebeveiliging verder te verbeteren. Ik denk dat het goed is om u daarover in ieder geval te informeren. Dat zal ik binnen een maand doen.

De **voorzitter**:
Prima. Dank u wel.