# 3
# Vragenuur: Vragen Rajkowski

Aan de orde is **het mondelinge vragenuur**, overeenkomstig artikel 12.3 van het Reglement van Orde.

**Vragen** van het lid Rajkowski aan de minister van Justitie en Veiligheid, bij afwezigheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties, over **het bericht "Russische en Chinese diensten gebruiken LinkedIn voor spionage bij Nederlandse bedrijven"**.

De **voorzitter**:
Aan de orde is het mondelinge vragenuur. Ik heet de minister van Justitie en Veiligheid van harte welkom. Ik vraag aan mevrouw Rajkowski van de VVD om haar mondelinge vraag te stellen aan de minister over het bericht "Russische en Chinese diensten gebruiken LinkedIn voor spionage bij Nederlandse bedrijven". Het woord is aan mevrouw Rajkowski. Gaat uw gang.

Mevrouw **Rajkowski** (VVD):
Dank u wel, voorzitter. Moet je je voorstellen: je zit in de kroeg een biertje te drinken, er komt iemand naast je zitten, diegene probeert erachter te komen waar je werkt en wat voor werk je doet, en achteraf kom je erachter dat het iemand is die is ingezet door de Russische of Chinese overheid en die jou informatie probeert te ontfutselen over jouw werk. Het kan toch niet waar zijn dat iedereen bang moet zijn voor iemand in de kroeg die een wodka bestelt? Dat klinkt misschien bizar, maar het gebeurt daadwerkelijk. Het is ogenschijnlijk onschuldig, maar het berichtje dat gister in het nieuws kwam, dat mensen via LinkedIn benaderd worden om hen op die manier informatie te ontfutselen, is ook zo'n voorbeeld.

Voorzitter. Via duizenden en allerlei verschillende soorten manieren worden heel veel Nederlanders dagelijks benaderd om hen informatie te ontfutselen. Iemand hoeft maar één keer niet scherp te zijn en het is prijs. De informatie die ze dan buit hebben gemaakt, zijn belangrijke dingen waar wij als Nederland ons brood mee verdienen. Wij maken in Nederland unieke chips. Wij doen de slimste dingen in de tuinbouw. Wij verdienen hier ons brood mee, en dan proberen zij ordinair te jatten. Dan denk je: goh, dat is vrij heftig; de straf die erop staat zal wel heel hoog zijn. Maar niets is minder waar. De straffen in Nederland gaan over tienduizenden euro's, en ondertussen kan diegene al in het vliegtuig naar China zitten. In andere landen liggen straffen veel hoger. Daar kan je er jarenlang de bak voor ingaan. Het probleem speelt niet alleen nu, maar ook over 50 jaar. Want als al onze kennis en informatie waar Nederland nu op draait worden gejat, wat doen wij over 50 jaar dan? Waar verdienen wij dan nog ons brood mee?

Voorzitter. Er zit maar één ding op. Wat de VVD betreft gaan we hoger straffen, moet de AIVD het aanpakken van dit soort praktijken topprioriteit maken en moeten we ervoor zorgen dat medewerkers en bedrijven beschermd worden en op de hoogte zijn van de risico's van hun vak. Laten we dit lopen, dan zullen we over een paar jaar moeten toekijken hoe ze in China met de kennis die wij hebben bedacht, die wij hebben gemaakt, hun brood verdienen. Onze economie is dan schade toegebracht en onze banen zijn weg.

Mijn vragen zijn de volgende. Is de minister het met de VVD eens dat het beschermen van onze bedrijven tegen buitenlandse spionage en jatwerk topprioriteit voor de AIVD moet zijn? Zo ja, welke stappen gaat de minister dan zetten om deze bedrijven beter te beschermen en onze kennis en technologie in huis te houden? Twee: is de minister het met de VVD eens dat dit soort praktijken zwaarder bestraft moeten worden? Zo ja, waar denkt de minister dan aan? Drie: klopt het ook dat de AIVD later deze week met een socialmediacampagne komt om de bewustwording te vergroten? Hoe gaat die eruitzien en is dat voldoende?

De **voorzitter**:
Dank u wel. Het woord is aan de minister.

Minister **Yeşilgöz-Zegerius**:
Dank u wel, voorzitter. Sorry, ik ben nog helemaal in de modus van verschillende vragen en dan in één keer beantwoorden. Ik wil mevrouw Rajkowski bedanken voor deze vraag, omdat ik nu nogmaals de gelegenheid krijg om aandacht te vragen voor dit belangrijke onderwerp. Dat doe ik mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties, die er nu niet bij kan zijn omdat ze in de Eerste Kamer zit. Bovendien kan ik aankondigen dat vandaag de AIVD-campagne "Check voor je connect" online gaat. Nederland is doelwit van spionage, zoals mevrouw Rajkowski al aangaf. Ons land heeft een open samenleving, een sterke economie en behoort tot de meest ontwikkelde, innovatieve landen ter wereld. Andere landen zijn geïnteresseerd in informatie over onze politieke, militaire en economische situatie en zijn actief op zoek naar wetenschappelijke en technologische kennis. Zoals de AIVD ook schrijft in de jaarverslagen: er wordt steeds meer digitaal gespioneerd. Dat is een feit.

Uit inlichtingenonderzoek blijkt dat inlichtingendiensten van andere landen ook steeds vaker social mediaplatforms gebruiken om nietsvermoedende gebruikers te rekruteren om informatie in te winnen. We hoorden net al enkele voorbeelden van hoe dat eruit kan zien. Gebruikers zijn zich daarvan vaak niet bewust en worden ongemerkt ingezet voor spionage. Het is een methode van buitenlandse inlichtingendiensten die in potentie massaal kan worden ingezet, al blijkt de benadering vaak wel specifiek op het eigen profiel van het doel gericht te zijn. Dat kan zijn op een specifiek werkveld, een specifiek kennisgebied of een specifieke expertise. De informatie die iemand zelf op internet heeft gezet, vormt daarbij het haakje voor een benadering.

Wanneer iemand een connectie accepteert, begint dat hele proces van iemand naar binnen trekken. Het begint met een uitnodiging om iets onschuldigs te schrijven of iets uit te zoeken wat gerelateerd is aan iemands expertise. Stap voor stap wordt een vertrouwensband opgebouwd, die leidt tot een aanbod voor een reis naar of een baan in het buitenland of tot het delen van info. Dus iedereen kan slachtoffer worden, en niet alleen mensen die werken met vertrouwelijke of gevoelige informatie bij bijvoorbeeld de overheid of techbedrijven. Zo kunnen bijvoorbeeld ook mensen die toegang hebben tot personeelsgegevens,

slachtoffer worden. Zij kunnen ook interessante doelwitten zijn. De voorbeelden zijn eindeloos.

Met de campagne "Check voor je connect" wil de AIVD mensen alert maken op onlinecontactverzoeken en hun handvatten bieden voor het herkennen van valse profielen. Ik denk dat het daarom heel goed is dat we hier vandaag staan. Dit is ook bewustwording. Dit is ook mensen scherp krijgen. Je hoeft inderdaad niet aan het hoofd van een bedrijf te staan of minister of Kamerlid te zijn; iedereen kan slachtoffer worden. Bewustwording is dus belangrijk. In de onlinecampagne wordt een en ander stap voor stap uitgelegd. Denk na. Is het logisch dat zo iemand mij benadert? Klinkt het te goed om waar te zijn? Dan is het waarschijnlijk te goed om waar te zijn. Het klinkt als een open deur, maar iedereen kan er zomaar mee te maken hebben.

Als het gaat over zware straffen denk ik dat het goed is om te doen wat in het coalitieakkoord staat en waarmee we nu ook bezig zijn op mijn ministerie: spionage strafbaar stellen. De voorstellen gaan binnenkort in consultatie. Ik kan de exacte termijn nog niet geven, maar op zeer korte termijn zullen ze worden gedeeld. Het lijkt me goed om dan stil te staan bij hoe het er uitziet: exact welke delicten en de strafmaat. Dat komt eraan. Ik denk dat ik mede namens mijn collega van Binnenlandse Zaken kan zeggen dat het onderwerp absoluut een heel hoge prioriteit heeft bij al onze inlichtingendiensten, ook de AIVD. We moeten ervoor zorgen dat we onze mensen en onze kennis en kunde goed beschermen.

Mevrouw **Rajkowski** (VVD):
Het is goed dat de minister zich op deze manier uitspreekt. De bewustwordingscampagne klinkt goed. Het gaat ons uiteindelijk ook om het volgende. We moeten ervoor zorgen dat mensen zich ervan bewust worden dat de strafbaarstelling er komt en dat de straffen echt hoog zijn. Het gaat hier om het brood dat wij met elkaar voor Nederland verdienen. Dagelijks worden duizenden Nederlanders via allerlei wegen benaderd. Onze banen en onze economie staan hier op het spel. Het gaat dus niet alleen om de statelijke actoren, maar ook om die indirecte wegen. Kan de minister dan ook toezeggen dat er straffen in de wet komen te staan die ook afschrikken, waardoor mensen denken "Nederland slaan we even over"?

Minister **Yeşilgöz-Zegerius**:
Ik kijk nu al uit naar dat debat, maar het moet inderdaad wel ergens over gaan. Je moet er wel voor zorgen dat het vervolgens ook echt die functie heeft. Laten we, zodra het op tafel ligt, met elkaar bekijken of het de juiste invulling is geweest. Ik denk dat wat hier wordt gezegd heel belangrijk is. Het raakt soms mensen thuis, soms burgers, soms bedrijven. Dat kan heel erg variëren. In de kern raakt het ons eigen verdienmodel en onze nationale veiligheid, dus dit is niet iets om klein te maken. Ik denk dat een campagne als Check before you connect ontzettend kan helpen bij dat scherpstellen, bij die bewustwording, ook bijvoorbeeld bij bedrijven. Als je merkt dat je hier slachtoffer van bent geworden, bijvoorbeeld doordat je bent ingegaan op een LinkedInverzoek waarop je niet had moeten ingaan — dat kan iedereen overkomen — is het goed om vervolgens aan te kloppen bij de veiligheidsafdelingen van je eigen bedrijf en meteen te zeggen: hé, volgens mij gaat hier iets mis. Daar zijn regels en protocollen voor. Er kan ook informatie worden ingewonnen op andere plekken via de AIVD. Ik denk dat we hier niet genoeg over kunnen spreken met elkaar.

Misschien mag ik er nog één ding aan toevoegen. Ik merk in mijn gesprekken met het bedrijfsleven, met kleine en grote bedrijven, dat er bij heel veel ondernemers een vorm van schaamte speelt. Op het moment dat er iets is gebeurd, of dat nou een hack is … Dat komt hier ook vaak langs in debatten. Hoe meer wij erover spreken en zeggen dat het iedereen kan overkomen, hoe makkelijker het hopelijk wordt om hulp te vragen. Bedrijven zijn ook bang om nog meer schade op te lopen als ze ermee naar buiten treden. Het is dus goed om hier te bespreken dat er een campagne is. Bij het debat over de strafbaarstelling van spionage komen we specifiek te spreken over de strafbaarstelling.

De **voorzitter**:
Tot slot, mevrouw Rajkowski.

Mevrouw **Rajkowski** (VVD):
Dank voor deze aanvullende informatie. Wij kijken ook uit naar het debat.

Als laatste zou ik het volgende willen meegeven. Als we überhaupt kijken naar het beschermen van onze Nederlandse bedrijven, zou het zo mooi zijn als de grotere bedrijven de kleine bedrijven waarmee ze samenwerken hierbij helpen, bijvoorbeeld als het gaat om bewustwordingscampagnes en masterclasses. Juist de kleine bedrijven hebben niet altijd de kennis en capaciteit om hiermee aan de slag te gaan, dus: groot helpt klein.

Minister **Yeşilgöz-Zegerius**:
Dat lijkt me een hele mooie oproep, die ik zal meenemen in de gesprekken die ik heb met het bedrijfsleven, met het mkb, VNO-NCW en iedereen. Het is een oproep waarbij ik me kan aansluiten.

De **voorzitter**:
Dank u wel, mevrouw Rajkowski. Er is een aantal vragen. Een vraag is een korte vraag zonder een uitgebreide inleiding. Ik geef als eerste het woord aan mevrouw Bromet van GroenLinks, dan aan mevrouw Dekker-Abdulaziz van D66 en dan aan de heer Ceder.

Mevrouw **Bromet** (GroenLinks):
Dit gebeurt nu in Nederland, maar het zal elders in Europa ook gebeuren. Spreekt de minister ook met haar collega's over deze kwestie en trekt ze samen met hen op?

Minister **Yeşilgöz-Zegerius**:
Dat is een goede vraag. Dit speelt absoluut in verschillende landen. Er zijn ook landen die een vergelijkbare campagne hebben opgezet. Think before you link is daar een voorbeeld van. Het speelt dus op meer plekken. Vanuit mijn rol als minister van Justitie en Veiligheid spreek ik inderdaad met mijn collega's over onderdelen van cybersecurity en cybercrime. Ik weet zeker dat mijn collega van Binnenlandse Zaken dat ook met haar collega's doet. Het staat absoluut op onze Europese agenda, maar ook breder.

Mevrouw **Dekker-Abdulaziz** (D66):
In Nederland hebben we een kenniseconomie die we moeten beschermen. Op dat punt ben ik het eens met de VVD. De AIVD vraagt meer bevoegdheden en data, maar je ziet dat spionage nog steeds ouderwets gebeurt door vertrouwen te winnen. Mijn vraag is: hoe worden de mensen met wie al contact is gelegd en die slachtoffer zijn geweest, actief ingelicht dat ze slachtoffer zijn geweest van spionage?

Minister **Yeşilgöz-Zegerius**:
Waar we het vandaag over hebben, is in die zin ietsje lastiger, want het gaat ook om de bewustwording van de persoon zelf, die op een gegeven moment denkt: wacht even, waar ben ik ingerold en waar ben ik in beland? Dan is het heel goed om meteen hulp te vragen, bijvoorbeeld via de afdeling binnen je eigen bedrijf of om je heen. Het hangt er natuurlijk vanaf in welke positie je bent benaderd. Maar inderdaad, als het om andere manieren gaat, zoals hacks en dergelijke, dan hebben we heel andere protocollen met elkaar opgesteld om ervoor te zorgen dat de juiste informatie op de juiste plek kan komen.

De **voorzitter**:
Dank u wel. De heer Ceder, ChristenUnie, en dan de heer Van Nispen, SP.

De heer **Ceder** (ChristenUnie):
Een zorgwekkend bericht. Ik vraag me af of de minister iets kan zeggen over de omvang van wat er al buit is gemaakt. Gaat het om financiën of om kennis? Zou de minister kunnen aangeven of het ook om informatie van de overheid gaat en van medewerkers die erbij betrokken zijn geweest?

Minister **Yeşilgöz-Zegerius**:
Zo heel specifiek heb ik die informatie niet. De AIVD en de inlichtingendiensten zijn er natuurlijk elke dag mee bezig, maar zij kunnen ook niet zo specifiek alle informatie volop met ons delen. Wel is het zo, zeker in het voorbeeld waarvoor we vandaag hier staan, dat het heel breed wordt uitgezet. Je ziet dat heel veel mensen benaderd worden. Dat kunnen er echt ongelofelijk veel zijn. Een deel daarvan reageert daarop. Uiteindelijk wordt het steeds kleiner en heb je een deel dat echt onderdeel hiervan wordt en op een gegeven moment merkt dat men informatie aan het delen is en bijdraagt aan zulke praktijken. Exacte cijfers hebben we niet. Ik heb gezien in de media dat er deskundigen zijn die zeggen dat het over duizenden mensen zou kunnen gaan. Ik heb begrepen dat de AIVD zegt: van dat getal schrikken we niet. Dus het ligt in die orde van grootte. Maar het begint echt met een veel grotere groep, dus dat betekent dat heel veel Nederlanders hiermee in aanraking kunnen komen.

De heer **Ceder** (ChristenUnie):
Het is denk ik wel goed om het scherp te hebben. Niet alleen om over hoeveel mensen het gaat — ik kan me inderdaad voorstellen dat het om duizenden mensen gaat — maar: bij hoeveel mensen is er inderdaad informatie weggeplukt, wat schadelijk kan zijn voor bedrijven of de overheid? Ik hecht er waarde aan als de minister misschien in een brief zou willen aangeven wat er is buitgemaakt. En alsnog de vraag: is er ook informatie van de overheid buitgemaakt?

Minister **Yeşilgöz-Zegerius**:
Welllicht is het een idee dat ik deze vraag doorgeleid naar mijn collega van Binnenlandse Zaken, die eigenlijk hier had moeten staan. Laat zij even kijken in hoeverre dit in een brief te vatten is.

De **voorzitter**:
Dat lijkt me een goede afspraak. Dan geef ik het woord aan de heer Van Nispen, SP.

De heer **Van Nispen** (SP):
Ik vind het ook terechte vragen. Ik zou het nog ietsje breder willen trekken. Recent waren er ook onthullingen over misbruik en spionage met behulp van Israëlische apparatuur. Nu weten we dat onze politie en de inlichtingendiensten ook gebruikmaken van Israëlische apparatuur, bijvoorbeeld het tapsysteem van de Nederlandse politie. De vraag is dus — en die ga ik ook stellen aan de minister: moeten wij ons zorgen maken over het gebruik van Israëlische apparatuur door onze politie en de inlichtingendiensten? Wat zijn op dit moment daarvan de risico's?

Minister **Yeşilgöz-Zegerius**:
Ik had kunnen weten dat deze vraag ook vandaag zou komen, maar ik heb deze vragen ook zelf uitgezet. Ik weet dat het op dit moment leeft. De heer Van Nispen en ik hebben volgende week een debat. Ik zou daar dan graag volgende week op willen terugkomen. Dan heb ik ook de informatie gekregen naar aanleiding van de vraag die ik heb uitgezet. Ik begrijp zijn zorgen, maar ik moet even toetsen wat we er nu precies van weten. We hebben volgende week een debat over de politie. Dus als de heer Van Nispen het goedvindt, neem ik het daarin mee.

De **voorzitter**:
De heer Van Nispen knikt.

De heer **Van Nispen** (SP):
Ja, voorzitter. Ik zou dan graag een brief willen ontvangen voor dat debat, zodat wij ons daarop goed kunnen voorbereiden.

Minister **Yeşilgöz-Zegerius**:
Dat doen we.

De **voorzitter**:
Dank. Dan wil ik de minister van Justitie en Veiligheid van harte danken. Ik schors voor een enkel moment en dan gaan we naar de tweede mondelinge vraag.

De vergadering wordt enkele ogenblikken geschorst.