Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

28 684 Naar een veiliger samenleving

Nr. 621 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 mei 2020

Inleiding

Tijdens het Algemeen Overleg strafrechtelijke onderwerpen op 17 april 2019 is gesproken over de vraag hoe we in het strafrecht kunnen ingrijpen tegen feiten die op of met behulp van het internet gepleegd worden, inclusief de Europese aanpak (Kamerstuk 29 279, nr. 517). Ik kondigde aan hier een brief over te sturen, en daarin tevens de dilemma's te schetsen waar de opsporing tegenaan loopt in de aanpak van internetcriminaliteit. Met deze brief voldoe ik aan die toezegging.

Allereerst wil ik de urgentie benadrukken die het bestrijden van deze vorm van criminaliteit voor mij heeft. In de huidige samenleving van digitalisering en connectiviteit zijn we altijd online. Dit heeft zijn weerslag op de manier waarop strafbare feiten worden gepleegd en op de manier waarop de aanpak vorm krijgt. Het is ook zichtbaar in de criminaliteitscijfers; daar waar in algemene zin de offline criminaliteit gestaag daalt, neemt de online criminaliteit toe. Ook daar waar een strafbaar feit in het fysieke domein is gepleegd, spelen het internet en de daarover gedeelde gegevens vaak een rol. Zij zijn dan ook vaste onderdelen geworden in opsporingsonderzoeken.

Ik richt mij in deze brief niet op alle aspecten van de aanpak, maar op enkele belangrijke hoofdpunten waar ik streef naar maatregelen die de mogelijkheden gaan verbeteren.

De urgentie wordt ook ingegeven door andere ontwikkelingen. Zo worden criminelen steeds slimmer. Was een poging tot oplichting een aantal jaren geleden nog relatief makkelijk te herkennen, inmiddels wordt dat steeds lastiger en wordt gebruik gemaakt van verfijndere methoden. Ook wijs ik

kst-28684-621
ISSN 0921 - 7371
's-Gravenhage 2020

op incidenten op het gebied van cybersecurity[1], die kwetsbaarheden in de maatschappij bloot leggen. In deze tijd van de coronacrisis, als gevolg waarvan mensen meer thuis zitten en meer gebruik maken van hun computer(verbindingen), zijn de eerste pogingen van criminelen om daar misbruik van te maken al direct zichtbaar geworden. Dit alles onderstreept de noodzaak om als maatschappij in staat te zijn deze criminelen op te sporen en hun activiteiten effectief aan te pakken. Zoals ik mijn brief aan uw Kamer van 23 april 2020[2] over corona en het justitie en veiligheid domein heb bericht, worden de ontwikkelingen in de criminaliteit in deze periode van de coronacrisis nauwgezet gevolgd. Op basis van de monitoring wordt met de betrokken partners gekeken of aanvullende interventies noodzakelijk zijn voor corona-specifieke criminaliteit zoals bijvoorbeeld phishing die inspeelt op corona. De politie hanteert al een brede bestrijdingsstrategie met publieke en private partners in de aanpak van cybercrime, met naast opsporing aandacht voor alternatieve interventies zoals preventie en verstoring. Deze wordt ook voor de actuele dreiging ingezet. Mijn handelen is er onder andere op gericht om preventie te versterken en de weerbaarheid van de samenleving te vergroten. Dat gebeurt niet alleen met publieke organisaties maar ook met private partijen, bijvoorbeeld zoals verenigd in het convenant «Eerst checken, dan klikken». Recentelijk is door een groot aantal organisaties aandacht geschonken aan voorkoming van slachtofferschap van cybercriminaliteit. In dit verband wijs ik graag op de website www.veiliginternetten.nl.

leeswijzer

In deze brief zal ik ingaan op enkele belangrijke dilemma's en op de consequenties wanneer de grootste knelpunten bij die dilemma's niet opgelost worden. Zo zal ik in deze brief ingaan op de relatie tussen de opsporing en het behouden van het open en vrije karakter van het internet. Dit geldt zowel voor de toegang daartoe als de bewegingsvrijheid er op, inclusief de bescherming van de privacy van gebruikers. Mijn inzet is er ten eerste op gericht om de online anonimiteit van verdachten van strafbare feiten zoveel mogelijk weg te nemen, zonder daarbij het open karakter van het internet aan te tasten. Ten tweede span ik mij, zowel op nationaal als op Europees en internationaal niveau, in voor het veilig gebruik van een open internet, onder andere door het schoonhouden daarvan, en aan een effectieve preventieve aanpak en opsporing van strafbare feiten. Dit is deels een klassieke opsporingstaak, maar gaat vaak ook in samenwerking met service providers en aanbieders van content[3], die hier ook een eigen maatschappelijke verantwoordelijkheid hebben. Die verantwoordelijkheid wordt steeds meer genomen, hetgeen ik toejuich. Daar waar dat niet geval is spreek ik hen er op aan en werk ik aan het uitbreiden van de wettelijke instrumenten, waarbij een goede balans moet worden gevonden tussen de belangen van alle betrokken partijen. Tot slot werk ik in internationaal verband aan het vergroten van de mogelijkheden om grensoverschrijdende opsporing in samenhang met andere landen te versnellen en te vergemakkelijken. Het grootste deel van het internetgebruik is inherent grensoverschrijdend van karakter en dit levert obstakels op voor de opsporing in Nederland, net zoals dat obstakels in andere landen oplevert.

---

[1] Zoals de recente problemen met Citrix
[2] Kamerstukken 35 300 VI en 25 295, nr. 126
[3] Zoals social media en andere aanbieders van diensten van de informatiemaatschappij zoals bedoeld in de richtlijn EU 2015/1535

In deze brief informeer ik u ook over de inzet van het kabinet bij de bitcoin problematiek naar aanleiding van een bericht daarover in de Telegraaf[4]. Daardoor voldoe ik tevens aan het verzoek van de vaste commissie voor Justitie en Veiligheid van 12 september 2019 hierover. Ten slotte ga ik in op een tweetal toezeggingen die ik heb gedaan tijden het AO Criminaliteitsbestrijding van 5 februari 2020 over de samenwerking tussen de politie en banken bij internetoplichting en de beperkingen waar partijen tegen aanlopen in het kader van de Algemene Verordening Gegevensbescherming (AVG) (Kamerstuk 28 684, nr. 617).

Enkele uitgangspunten

In discussies over internetcriminaliteit en de opsporing in het digitale domein blijkt dat volgens sommigen in de digitale wereld fundamenteel andere uitgangspunten gelden dan in de fysieke wereld, bijvoorbeeld op het gebied van anonimiteit en privacy. Ik ben die mening niet toegedaan. Het inherent grenzeloze karakter van internet in relatie tot het kader van de territoriaal geclausuleerde soevereine rechten voor strafrechtelijke handhaving vraagt weliswaar om een andere en meer internationale aanpak, maar de onderlinge principes zijn dezelfde[5]. Een voorbeeld van zo'n andere aanpak is het verwijderen van strafbaar materiaal. In de fysieke wereld kan dat door bijvoorbeeld een papieren foto te vernietigen. In de digitale wereld zou diezelfde foto waarschijnlijk op veel meer plekken zijn opgeslagen, is de infrastructuur van internetbedrijven betrokken, en moeten persoonsgegevens worden vastgelegd en communicatiepaden tussen computers ontoegankelijk worden gemaakt.

Ik hanteer daarom een aantal uitgangspunten voor de rechtshandhaving die zowel in het fysieke als in het digitale domein dienen te gelden:

1. Belangen zoals rechtshandhaving, privacy, economie en veiligheid zijn allen legitiem en zijn geen van allen absoluut.
2. De overheid accepteert geen vrijplaatsen voor criminelen.
3. Het strafrecht wordt, binnen de beschikbare middelenmix, als optimum remedium ingezet.
4. Regelgeving dient handhaafbaar en uitvoerbaar te zijn.

Deze uitgangpunten kunnen helpen bij het overdenken van hieronder verder uitgewerkte thema's en in het bijzonder voor het maken van keuzes in het digitale domein. En daarbij blijkt dat er niet altijd pasklare antwoorden zijn, maar tenminste wel meer of minder ontwikkelde ideeën over een verantwoorde en effectieve aanpak van internetcriminaliteit en van opsporing in de huidige digitale tijd. Hieronder ga ik vanuit dit vertrekpunt nader in op drie hoofdthema's, en tevens hoofddilemma's, die ik in deze brief wil aansnijden.

Thema 1: Het open karakter van het internet, privacy en opsporingsbevoegdheden

Een van de thema's die centraal staan betreft de verhouding tussen het open karakter van het internet, de daarbij behorende privacy en het anoniem bewegen op het net alsmede de belangen van de aanbieders, en de verhouding met de maatschappelijke wens om effectief misdaad te kunnen bestrijden. Deze elementen en de spanning die daartussen bestaat, komen hieronder aan de orde. Bij deze elementen speelt tevens mee dat het internet een internationaal karakter heeft. Dit komt bij thema 3 separaat aan de orde.

---

[4] https://www.telegraaf.nl/entertainment/2139358386/john-de-mol-vraagt-alsnog-vonnis-tegen-facebook

[5] Kamerstukken 33 694 en 26 643, nr. 47

Het internet is een digitale wereld waarin ontelbare (en een groeiend aantal) apparaten, netwerken, personen, bedrijven en organisaties met elkaar verbonden zijn. Hierdoor kunnen personen grote hoeveelheden gegevens gemakkelijk, direct en snel ontsluiten, delen en vastleggen. Ook stelt het organisaties en personen in staat allerlei transacties af te wikkelen. In de kern is het internet een vrije omgeving: het «is» niet van iets of iemand. De Nederlandse regering heeft in 2016 aangegeven zich te richten op het benutten van kansen die het internet biedt voor innovatie en economische groei en op het garanderen van veiligheid en mensenrechten in het cyberdomein. Reeds in deze brief heeft het kabinet laten zien zich sterk te willen maken voor de drie kernelementen: een open, vrij en veilig internet[6]. Dit is herhaald in de recente AIV-aanvraag over regulering van online content[7]. Daarbij gaat het niet alleen om de toegankelijkheid tot het internet, maar ook het recht om zich daar in beginsel vrij te kunnen bewegen zonder dat de overheid dit beperkt. Naast het belang van de openheid en vrijheid wordt daarin gewezen op de risico's die ontstaan voor de veiligheid, en wordt advies gevraagd over opties voor regulering van content op het internet door overheden. Wanneer dat advies ontvangen is, zal het kabinet bezien wat de mogelijkheden zijn.

Een van de belangrijkste en tevens lastigste elementen in het bestrijden van internetcriminaliteit is echter het achterhalen van de identiteit van een verdachte. De technologie maakt het mogelijk dat personen online (nagenoeg) anoniem kunnen bewegen, met name door het gebruiken van aliassen en technische afschermingsmaatregelen. Dit draagt bij aan de beveiliging van informatie die in het digitale domein wordt verspreid. Deze beveiliging is cruciaal voor vertrouwelijke communicatie tussen overheid, bedrijf en burger. Maar tezamen maken zij het achterhalen van de identiteit van verdachten wel moeilijker. Dit wordt verder versterkt door de inherente grenzeloosheid van het internet en de schaalgrootte die is bereikt als gevolg van de digitale revolutie, als gevolg waarvan ook kwaadwillenden snel, anoniem, en verstopt tussen miljarden gegevensuitwisselingen, activiteiten kunnen ontplooien. In de gedigitaliseerde maatschappij worden terecht hoge eisen gesteld aan het waarborgen van de privacy van personen. Aan de andere kant heeft de samenleving behoefte aan en recht op een veilige samenleving en bescherming van (kwetsbare) personen en goederen. Ook op het internet. Dit is een inherent dilemma van het internet.

Dit dilemma speelt ook een grote rol bij het bepalen van een standpunt over encryptie. Het kabinet Rutte II heeft hierin een kabinetsstandpunt ingenomen dat nog steeds staand beleid is. Het gaat hier om de onwenselijkheid van het nemen van beperkende wettelijke maatregelen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland.[8] Tegelijkertijd heb ik zorg, zeker ook naar de toekomst, over de mogelijkheden om effectief op te sporen. Naast andere, overigens steeds vernieuwende, mogelijkheden voor personen om hun identiteit te verhullen, maakt encryptie het voor politie en justitie feitelijk moeilijk zicht te hebben op gegevens met betrekking tot strafbare feiten en om de herkomst van gegevens te herleiden naar personen die mogelijk bij strafbaar handelen zijn betrokken of daarvan weet hebben. Daardoor is het zeer geregeld niet mogelijk opsporingsonderzoeken op te starten of na verloop van enige tijd bewijs rond strafbare feiten te verkrijgen. Naar aanleiding van een aankondiging van een groot internationaal social

---

[6] Kamerstuk 26 643, nrs. 411 en 383

[7] https://www.adviesraadinternationalevraagstukken.nl/documenten/adviesaanvragen/2019/05/27/adviesaanvraag-regulering-van-online-content

[8] Kamerstuk 26 643, nr. 383

media bedrijf om over te gaan op end-to-end encryptie (E2EE), is in het najaar van 2019 opnieuw discussie ontstaan. Zoals gemeld in eerdere Kamervragen van het lid Verhoeven wordt samen met publieke en private belanghebbenden geïnventariseerd hoe rechtmatig toegang kan worden verkregen tot versleuteld bewijs. Ik streef naar oplossingen binnen de kaders van het kabinetsstandpunt die recht doen aan de belangen van de opsporing en de nationale veiligheid[9]. In de aanpak van online seksueel misbruik van kinderen wordt hierbij onder andere gedacht aan crawling technieken of screening van gegevens voordat gegevens kunnen worden geupload («photo DNA»). Het spreekt voor zich dat daarbij de fundamentele rechten conform daarvoor bestaande wettelijke kaders moeten worden geborgd.

In algemene zin betekent dit dat mijn inspanningen er op zijn gericht om, binnen de grenzen van de rechtsstaat, waaronder verdragsrechtelijke normen, de opsporing optimaal te voorzien van bevoegdheden die nodig zijn om strafbare feiten te onderzoeken, daders voor de rechter te krijgen en daardoor in te staan voor de veiligheid van de samenleving en de bescherming van personen en goederen.

Het vorig jaar in werking getreden wetsvoorstel Computercriminaliteit III is een voorbeeld van de afweging van het opsporingsbelang, het privacy belang en het open karakter van internet. In het wetgevingsproces is deze spanning uitvoerig besproken. Het toont aan dat het introduceren van nieuwe bevoegdheden die passen bij de nieuwe technologische werkelijkheid mogelijk is, met inachtneming van de privacy van internetgebruikers in het algemeen. In de volgende thema's worden andere ontwikkelingen genoemd waarin eveneens stappen worden gezet voor nieuwe mogelijkheden in het bestrijden van internetcriminaliteit.

Samenvattend:
– Als het AIV-rapport over regulering van online content er is, komt het kabinet met een standpunt.
– Samen met publieke en private belanghebbenden inventariseert mijn ministerie welke mogelijkheden er, binnen de kaders van het kabinetsstandpunt, zijn om toegang te krijgen tot versleuteld bewijs.

Thema 2 de rol van service providers, social media en andere aanbieders van diensten van de informatiemaatschappij

De digitale revolutie heeft, naast de hierboven genoemde aspecten, nog andere grote veranderingen gebracht. Een daarvan is de positie die service providers, (aanbieders van) social media, en andere aanbieders van diensten hebben. Zij hebben een sleutelrol als het gaat om de infrastructuur van de moderne informatiemaatschappij, en hebben ook een bijzondere positie ten aanzien van de gegevens die over hun netwerken verspreid worden. Zeker als dat gegevens zijn die direct of indirect te maken hebben met strafbare feiten.

Strafbaar gedrag in een online omgeving is een maatschappelijk probleem dat deels vanuit de overheid, maar ook vanuit de samenleving zelf moet worden aangepakt. In de inleiding noemde ik al de samenwerking die er is met bedrijven. Dit is onder meer nodig wegens de positie van ons land: Nederland heeft één van de grootste internetknoop-punten ter wereld, een omvangrijke infrastructuur, en een bijzonder grote hostingsector. Dat schept niet alleen een bijzondere verantwoordelijkheid voor de Nederlandse overheid, maar ook voor het bedrijfsleven, om misbruik van internetvrijheden tegen te gaan op een manier die past bij

[9] Aanhangsel Handelingen II 2019/20, nrs. 758 en 1095

hun rol als ondernemer en met inachtneming van de rechten en vrijheden van hun klanten. Het tegengaan van strafbaar gedrag is een gedeeld belang van alle partijen. Het moet vanzelfsprekend worden dat we met een actieve, open houding, publiek en privaat, ons gezamenlijk verantwoordelijk voelen voor het bestrijden van misbruik van internetvrijheden. Zowel op nationaal als op Europees en internationaal niveau span ik mij in om bedrijven optimaal te laten bijdragen aan het veilig gebruik van een open internet.

Grote internationale platforms en dienstenaanbieders bedienen niet alleen de Nederlandse markt, maar vaak meerdere landen, en in veel gevallen zelfs de hele wereld. Het uitoefenen van invloed op deze grote spelers is nodig om, bij het nastreven van de genoemde doelen, resultaat te boeken. Vanuit Nederland is deze invloed echter beperkt. De bedrijven zijn gevestigd in andere landen, vallen onder andere (of meerdere) rechtsregimes, en ook de relevante gegevens bevinden zich vaak niet in Nederland. Om toch de gewenste invloed uit te oefenen, moet daarom internationaal en Europees samenwerking worden gezocht. Dat is echter een langdurig proces, waarbij belangen van meerdere landen meegewogen worden. Binnen dit thema is dit een kerndilemma; de keuze voor een lang proces met onzekere uitkomst is soms echter nodig.

Mijn aanpak bestaat daarom uit twee lijnen. In de eerste plaats streef ik na om binnen Nederland te doen wat er mogelijk is. Deze aanpak bestaat uit het maximaal gebruik maken van de bestaande bevoegdheden, zoals het geven van een bevel tot ontoegankelijkmaking van gegevens, of het vorderen van gegevens die aanwezig zijn bij social media. Binnen de Nederlandse rechtsmacht kan dat rechtstreeks, en buiten de Nederlandse rechtsmacht door rechtshulpverzoeken en operationele samenwerking. Daarnaast bestaat mijn aanpak uit het vinden van nieuwe mogelijkheden op het terrein van samenwerking en regelgeving, die verder bevorderen dat opgetreden kan worden tegen strafbare feiten die op of met gebruikmaking van het internet worden gepleegd.

Binnen Nederland is een belangrijk voorbeeld hiervan mijn strijd tegen online seksueel kindermisbruik (kinderporno). Hier heb ik een aanpak geïntroduceerd die zich richt op het voorkomen van slachtofferschap (preventie), het schonen van internet en het versterken van de opsporing. Deze aanpak bestaat ten eerste uit een publiek-private samenwerking voor het snel verwijderen van kinderporno en het maken van een onafhankelijke monitor om meldingen van kinderporno te volgen en inzichtelijk te maken welk bedrijf hoeveel meldingen krijgt. Daarnaast heeft de politie met het meldpunt kinderporno een hash-check-service gebouwd, waarmee bedrijven zelf hun servers kunnen scannen en schonen van kinderporno. En zelf heb ik een wetgevingstraject gestart om, bij bedrijven die na een melding kinderporno niet accuraat van hun server verwijderen, de verwijdering van kinderporno middels het bestuursrecht af te dwingen. Inzet en actie hierop zal in de toekomst niet meer vrijblijvend zijn, maar met herstelsancties worden afgedwongen[10].

De tweede lijn is het streven van het kabinet in Europees en internationaal verband om de bedrijven maximaal mee te laten werken aan het schoonhouden van het internet en aan een effectieve opsporing. In algemene zin geldt dat er steeds meer regels komen waar zij zich aan moeten houden. Dit is een gevolg van nationaal beleid van verschillende landen, maar zeker ook van internationale samenwerkingsverbanden,

[10] Kamerstuk 31 015, nr. 175

zoals de EU. Nederland stelt zich daar actief bij op. Ook social media zelf spreken zich uit, Facebook heeft ook zelf opgeroepen tot meer regulering[11].

Een goed voorbeeld is de bestrijding van online hatespeech. Waar in Europees verband wordt ingezet op gedragscodes en concrete afspraken met IT-bedrijven over registratie, beoordeling en verwijdering – waar nodig met aanvullende wet- en regelgeving – vult het kabinet dat in Nederland aan met projecten die zijn gericht op bewustwording, waarbij internetgebruikers een handelingsperspectief wordt geboden indien zij online met hatespeech worden geconfronteerd.

Een ander dilemma dat is gerelateerd aan de rol van dienstverleners, betreft de zogenoemde «Over The Top» diensten, afgekort OTT. Dit zijn diensten die vertrouwelijke telecommunicatie tussen individuele gebruikers mogelijk maken, zoals WhatsApp of internettelefonie. Deze communicatie verloopt via het internet en wijkt daarmee af van de traditionele telefonie, die via de daarvoor gebruikelijke infrastructuur verloopt. Voor de opsporing is dit vooral relevant omdat de verplichting om de telecommunicatie aftapbaar te maken (een verplichting op grond van de Telecommunicatiewet) niet geldt voor OTT-diensten. Het effectief invoeren van een dergelijke verplichting is niet eenvoudig en vergt nadere uitwerking. Hierbij moet aandacht worden besteed aan het feit dat veel OTT-diensten worden aangeboden door bedrijven die niet in Nederland gevestigd zijn. Dit zou een bevoegdheid tot grensoverschrijdend vorderen kunnen betekenen, waar bij ook aandacht moet worden besteed aan handhaving. Ook gebruiken meerdere OTT-diensten end-to-end versleuteling waardoor voor effectieve toegang tot deze versleutelde data de voortgang van de in relatie tot encryptie bovengenoemde inventarisatie van belang is.

Samenvattend:
– Binnen Nederland strijd ik tegen online seksueel misbruik van kinderen middels een publiek-private samenwerking
– In Europa zetten we in op regelgeving om bedrijven bij te laten dragen aan het schonen van het internet en aan opsporing, zoals bij hatespeech. Binnen Nederland vult het kabinet dat aan met bewustwordingsprojecten.
– Ik onderzoek de mogelijkheden van toegang tot communicatie via OTT-diensten.

Thema 3 grensoverschrijdend karakter van het internet

In het vorige thema is reeds ingegaan op nationale en internationale maatregelen die erop gericht zijn om de rol en verantwoordelijkheden van bedrijven te verduidelijken en te verstevigen, en bovendien de mogelijkheden voor opsporingsautoriteiten om voor de opsporing relevante gegevens te verkrijgen bij die bedrijven. Bedacht moet worden dat het internet inherent grensoverschrijdend is. Bij de hiervoor gegeven voorbeelden is al aangegeven dat maatregelen jegens bedrijven ook en soms zelfs primair op internationaal niveau moeten worden genomen.

Het centrale dilemma op dit terrein ligt op het punt van jurisdictie om opsporingshandelingen in te zetten die zich ook kunnen uitstrekken tot andere landen. Het inzetten van bevoegdheden is immers beperkt tot situaties en omgevingen waar Nederlandse opsporingsambtenaren jurisdictie hebben. Andersom is dit ook zo; buitenlandse opsporingsambtenaren moeten zich, bij het doen van onderzoek buiten hun rechtssfeer,

[11] Washington Post, 29 maart 2019

ook houden aan de randvoorwaarden van de soevereiniteit van andere landen, in wiens omgeving zij onderzoek willen doen[12].

Voor het doen van onderzoek zijn verschillende instrumenten beschikbaar. In sommige gevallen is de soevereiniteit van andere landen niet in het geding, bijvoorbeeld wanneer het publiek toegankelijke gegevens betreft. In andere gevallen zijn instrumenten voorhanden als rechtshulpverzoeken en sinds enkele jaren binnen de EU het Europees opsporingsbevel (EOB). Zoals ook met uw Kamer besproken in verschillende overleggen over de inmiddels ingevoerde Wet Computercriminaliteit III komt het verder voor dat – ondanks redelijke inspanning – onbekend is in welk land een bepaalde gegevensdrager zich bevindt (loss of location), terwijl via het internet wel de verbinding met het desbetreffend geautomatiseerd werk bekend is. Er kan dan dus ook geen rechtshulpverzoek worden ingediend, terwijl strafrechtelijk optreden wel wenselijk is. Daarin gesteund door de inhoudelijke discussie bij de behandeling van het wetsvoorstel Computercriminaliteit III stel ik mij nog steeds op het standpunt dat in dergelijke gevallen optreden mogelijk is. Dat wordt echter begrensd door het lopende het onderzoek verwerven van informatie over het land waarin de doelcomputer zich bevindt. Alsdan moet alsnog contact met dat land worden opgenomen en worden overlegd over rechtshulp. Het openbaar ministerie heeft dit bij de inwerkingtreding van de genoemde wet vastgelegd in een beleidsregel[13].

In 2016 heeft het Nederlandse voorzitterschap van de raad JBZ van de Europese Unie het initiatief genomen om te komen tot Europese regels op het terrein van het rechtstreeks, grensoverschrijdend vorderen van elektronisch bewijs bij internetdienstverleners, ook wel E-evidence genoemd. Steeds meer data die relevant is voor opsporingsonderzoeken in Nederland zijn in beheer bij bedrijven buiten Nederland. Hierbij spelen veel en grote belangen. In de eerste plaats betekent de bevoegdheid om rechtstreeks in andere landen elektronisch bewijs te kunnen vorderen, dat andere landen dat ook in jouw eigen land kunnen doen. Het dilemma bestaat dan dus uit de spanning tussen enerzijds de wens om snel grensoverschrijdend onderzoek te doen, afgezet tegen de omstandigheid dat er dan direct onderzoek gedaan kan worden in de rechtssfeer van andere soevereine staten. Rechtstreeks onderzoek doen heeft immers gevolgen voor de controle op en het overzicht over de activiteiten van andere landen op het, in ons geval, Nederlandse grondgebied. Ook moeten er goede afspraken gemaakt worden over de strafbare feiten waarbij van deze bevoegdheid gebruik gemaakt kan worden, alsmede stevige waarborgen. De onderhandelingen over een verordening zijn nog gaande. In december 2018 heeft de raad JBZ zijn positie over de voorgestelde verordening vastgesteld. In het begin van 2020 kan worden verwacht dat het Europees Parlement een positie bepaalt over de door de Commissie voorgestelde verordening. Vervolgens zal een triloog nodig zijn. Volgens de vaste praktijk EU Raden zal de Kamer via geannoteerde agenda's en verslagen op de hoogte worden gehouden van de verdere ontwikkelingen.
Nederland heeft in de raadsonderhandelingen als leidraad gehanteerd dat een E-evidence bevoegdheid noodzakelijk is en gepleit voor evenwichtige wetgeving die effectief is en fundamentele rechten respecteert. Ik zal dit uitgangspunt blijven uitdragen. De spanning tussen enerzijds de wens om rechtstreeks onderzoek te kunnen doen en anderzijds de noodzaak van het hanteren van goede waarborgen komt hier rechtstreeks naar voren:

---

[12] Kamerstukken 33 694 en 26 643, nr. 47
[13] Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126NBA SV, nr. 2019A001, van 1 maart 2019

Nederland heeft in de JBZ-raad tegen de algemene oriëntatie gestemd vanwege het ontbreken van voldoende waarborgen.

Ook stelt Nederland zich actief op bij de onderhandeling rondom het gewenste tweede aanvullende protocol bij het cybercrime verdrag. Doel is om hierin ook afspraken te maken over directe grensoverschrijdende samenwerking tussen rechtshandhavingsautoriteiten en dienstverleners, maar dan breder dan de EU. Die afspraken zouden de praktijk, waarin bijvoorbeeld via een netwerkzoeking[14] opsporingsonderzoek wordt uitgevoerd als niet duidelijk is dat gegevens in een andere jurisdictie zijn, wettelijk schragen. In het geval tijdens onderzoek blijkt dat die gegevens zich niet binnen de Nederlandse rechtsmacht bevinden, kan op dat moment met de autoriteiten van een ander land alsnog samenwerking (rechtshulp) worden gezocht.

Een laatste aspect dat ik wil noemen in dit verband is de situatie waarin er verschillen zijn in wetgeving die het aantrekkelijk maken om producten via het internet te bestellen in landen waar dat legaal is, om ze per post te laten bezorgen in landen waarin dat strafbaar is. Dit specifieke thema is aan bod gekomen in de vragen van het lid Kuiken[15] over het via internet (legaal) kopen van bepaalde typen drugs en wapens in het buitenland, om ze vervolgens illegaal in Nederland te laten bezorgen. In aanvulling op hetgeen in antwoord op deze vragen is vermeld, kan ik u melden dat de Staatssecretaris van Volksgezondheid, Welzijn en Sport (VWS) en ik een wetsvoorstel in voorbereiding hebben om de problematiek van Nieuwe Psychoactieve Stoffen (NPS) aan te pakken. Hier gaat het om drugs die sterk lijken op stoffen die al via de Opiumwet verboden zijn en een vergelijkbare werking hebben. Veel andere landen hebben al wetgeving die dergelijke stoffen verbiedt, wat Nederland tot een productieland van NPS heeft gemaakt. De NPS zijn vaak gewoon op het open internet te bestellen. Met het genoemde wetsvoorstel worden deze stoffen ook in Nederland verboden, en kan er tegen handelaren worden opgetreden. Nederland volgt hierbij de systematiek die ook in Duitsland en België wordt gehanteerd. Het wetsvoorstel is begin 2020 in consultatie gegaan.

Samenvattend:
– Het kabinet zet binnen de EU in op een effectieve E-evidence bevoegdheid, met goede waarborgen.
– Het kabinet zet in op een tweede aanvullend protocol bij het cybercrime verdrag, ter bevordering van directe grensoverschrijdende opsporing, ook buiten de EU.
– Het kabinet heeft een wetsvoorstel in voorbereiding voor de aanpak van de problematiek van Nieuwe Psychoactieve Stoffen.

Bitcoinfraude

De vaste commissie voor Justitie en Veiligheid heeft mij bij brief van 12 september 2019 verzocht om de Kamer te informeren over de inzet van het kabinet bij de bitcoinproblematiek naar aanleiding van een bericht daarover in de Telegraaf[16]. Bij genoemde bitcoinproblematiek gaat het om een vorm van beleggingsfraude waarbij mensen via valse of misleidende advertenties op o.a. social media en websites verleid worden om te beleggen in vaak niet-bestaande bitcoins. Hierbij wordt soms gebruik gemaakt van bekende Nederlanders, die het product zogenaamd

[14] Het doorzoeken van op het doorzochte geautomatiseerd werk (bijvoorbeeld een computer) aangesloten andere componenten, zoals mogelijke opslag van gegevens in de cloud.
[15] Aanhangsel Handelingen II 2019/20, nr. 3401
[16] https://www.telegraaf.nl/entertainment/2139358386/john-de-mol-vraagt-alsnogvonnis-tegen-facebook

aanprijzen. Vervolgens worden slachtoffers naar websites geleid om gegevens af te staan en geld te betalen. Bij de aanpak van deze vorm van oplichting spelen alle thema's en dilemma's die ik hiervoor heb omschreven een rol: criminelen die zich overal ter wereld kunnen bevinden maken gebruik van het open karakter van het internet om zoveel mogelijk willekeurige slachtoffers te maken. Ook deze vorm van grensoverschrijdende oplichting is lastig aan te pakken. De rol van service providers en (grote) social media en andere private partijen is hierbij van groot belang.

Daarbij geldt, zoals ik al meermaals met uw Kamer heb besproken, dat de meest effectieve manier om fraude – en zeker deze vorm van fraude – aan te pakken is het voorkomen daarvan. Mensen moeten zich daarom steeds bewust zijn van de risico's die aan de orde kunnen zijn bij dit soort aanbiedingen op internet of anderszins en zich heel goed informeren voordat men op zo'n aanbieding ingaat. Diverse publieke en private partijen, zoals politie, ACM, AFM en Fraudehelpdesk, waarschuwen ook regelmatig voor dit soort fraude en fraudeurs. Daarnaast geef ik steeds aan dat ook private partijen, zoals in dit geval bijvoorbeeld de (grote) social media bedrijven, een eigen verantwoordelijkheid ten aanzien van het voorkomen van criminaliteit hebben.

In antwoord op eerdere schriftelijke vragen van uw Kamer heb ik aangegeven[17] op welke wijze de problematiek van valse advertenties voor bitcoins kan worden aangepakt. Zo heb ik onder andere aangegeven dat er – als er bij dit soort advertenties sprake is van het vermoeden van een strafbaar feit, zoals oplichting – aangifte kan worden gedaan bij de politie. De politie zal onderzoeken of de zaak voldoende opsporingsindicaties bevat om tot een succesvolle opsporing en vervolging te kunnen leiden. In mijn brief over boilerroombeleggingsfraude[18] ben ik ingegaan op het internationale en dynamische karakter van dit soort vormen van fraude, die de opsporing daarvan niet eenvoudig maakt.

Het kabinet heeft op 11 december 2019 een wetsvoorstel in consultatie gebracht ter implementatie van de Europese richtlijn[19] waarin fraude met digitale betaalmiddelen, waaronder bitcoins, apart strafbaar wordt gesteld en waarop hogere straffen komen te staan.

In het geval van misleiding kan de consument zich ook beroepen op de regels met betrekking tot oneerlijke handelspraktijken. Personen van wie de naam of beeltenis wordt misbruikt, kunnen hierover klagen bij de desbetreffende (social) media platforms en hen verzoeken hun naam of beeltenis te verwijderen. Als aan dit verzoek niet wordt voldaan kan dit voorgelegd worden aan de civiele rechter.

Onlinehandelsfraude

De meeste van de hierboven genoemde punten die gelden voor bitcoinfraude gelden ook voor onlinehandelsfraude. Ik doel hierbij onder andere op het grensoverschrijdende karakter, het belang van preventie, het doen van aangifte en de gevolgen voor het slachtoffer. Ik ben in mijn brieven van 5 april 2019 en 15 november 2019[20] uitgebreid ingegaan op de aanpak van internetoplichting en de rol van banken hierin. Dit is ook aan de orde gekomen tijdens het AO Criminaliteitsbestrijding van 5 februari 2020

---

[17] Aanhangsel Handelingen II 2018/19, nr. 3415

[18] Kamerstuk 29 911, nr. 199

[19] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/12/11/mvt-wetsvoorstel-implementatie-van-de-richtlijn-2019–713-eu-van-het-europees-parlement-en-de-raad-over-bestrijding-van-fraude-met-en-vervalsing-van-niet-contante-betaalmiddelen

[20] Kamerstuk 29 911, nrs. 237 en 260

(Kamerstuk 28 684, nr. 617). Mevrouw van Toorenburg (CDA) heeft toen aangegeven graag te zien dat de politie samen met de banken slachtoffers vaker helpt. Ik heb hierover op 11 maart 2020 gesproken met de voorzitter van de Nederlandse Vereniging van Banken (NVB), de heer Buijink. De heer Buijink heeft tijdens dit gesprek aangegeven dat er gesprekken zijn gestart tussen de banken, de politie, het Landelijk Meldpunt Internetoplichting (LMIO) en het openbaar ministerie. Afgesproken is dat de volgende thema's nader zullen worden uitgewerkt:

1) Preventie/communicatie (bijvoorbeeld gericht op geldezels).
2) Het bekijken van mogelijkheden om de gegevensdeling tussen politie en de banken in het kader van de LMIO, uit te breiden. Een ander thema dat verkend wordt is informatiedeling tussen banken en politie over katvangers.
3) Checkfunctie 2.0, hierbij gaat het bijvoorbeeld om transacties waarbij een tussenpartij (payment service provider) betrokken is. Door het zichtbaar maken van de naam van de eindbegunstigde (degene voor wie uiteindelijk het geld bestemd is), wordt de transparantie verhoogd.
4) Interventies door banken en politie met aandacht voor slachtoffers in de vorm van gesprekken met «startende» fraudeurs en ingrijpen.

Tijdens het AO Criminaliteitsbestrijding is ook gesproken over de beperkingen waar partijen tegen aanlopen in het kader van de Algemene Verordening Gegevensbescherming (AVG). Dit punt wordt door partijen meegenomen in het thema gegevensdeling/gegevensuitwisseling.

Op het moment dat de verschillende thema's door partijen in detail zijn uitgewerkt, dient onderzocht te worden of de geïdentificeerde maatregelen ook praktisch en juridisch (onder andere met het oog op de privacyregels) haalbaar zijn. Partijen hebben aangegeven dat de gesprekken door de maatregelen rondom het coronavirus tijdelijk stil zijn komen te liggen, maar dat de gesprekken weer worden gestart zodra dit mogelijk is. Ik zal uw Kamer over de uitkomsten informeren.

Tot slot

Het voorkomen en bestrijden van internetcriminaliteit is in veel gevallen een complexe aangelegenheid. Zowel op bestuurlijk als op uitvoerend niveau zet de Nederlandse overheid, in het bijzonder de opsporingsdiensten, zich daarvoor met hoge prioriteit in. De Nederlandse overheid is echter niet de enige partij die invloed uitoefent op de relevante spelers. Private partijen spelen, zowel zelfstandig als in samenwerking met de overheid, een belangrijke rol. En ook in Europees en internationaal verband werkt Nederland actief samen om de mogelijkheden voor preventie en opsporing te verbeteren. In deze brief heb ik de belangrijkste dilemma's genoemd, maar aan het eind van elk van de betreffende hoofdstukken ook aangegeven welke belangrijke initiatieven ik heb lopen. Ik zal mij daar, in deze internationale omgeving met een veelheid aan belangen, onverminderd voor in blijven zetten.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus