Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

35 656 Implementatie van Richtlijn 2019/713/EU van het Europees Parlement en de Raad van 17 april 2019 betreffende de bestrijding van fraude met en vervalsing van niet contante betaalmiddelen en ter vervanging van Kaderbesluit 2001/413/JBZ van de Raad (PbEU L 123/18)

Nr. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 28 januari 2021

I ALGEMEEN DEEL

1. Inleiding

Met veel belangstelling heb ik kennisgenomen van het verslag van de vaste commissie voor Justitie en Veiligheid. Het verheugt mij dat de meeste fracties steun uitspreken voor het wetsvoorstel. Ik dank de leden van de verschillende fracties voor de door hen gestelde vragen, die ik hierna graag beantwoord. Bij de beantwoording is de indeling van het verslag zoveel mogelijk gevolgd.

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel. Zij vinden het ook wenselijk dat fraude, waaronder digitale fraude, hard wordt aangepakt. Met deze leden ben ik van mening dat in een wereld waar digitalisering steeds meer geïntegreerd raakt in het dagelijks leven het noodzakelijk is ook op dit gebied efficiënte strafrechtelijke bescherming te bieden. Deze leden nemen dan ook met genoegen kennis van de verhoging de strafmaat in artikel 138c Sr. De nadere vragen die zij stellen over dit onderwerp beantwoord ik graag in het Artikelsgewijs deel van deze nota.

Terecht merken de leden van de VVD-fractie op dat de richtlijn in vrij algemene bewoordingen is gesteld. Daarmee wordt beoogd een «helder, robuust en techniekneutraal – en daarmee toekomstbestendig – verplichtend kader» op te stellen. Op de vraag van deze leden of de regering dit ziet als een voordeel of een nadeel voor vervolging van criminele activiteiten kan ik als volgt antwoorden. Fraude met en vervalsing van niet-contante betaalmiddelen kent een steeds sterkere digitale component. De innovatie op velerlei gebieden, waaronder betaaltechnologieën, is sterk toegenomen. Nieuwe betaaltechnologieën betekenen ook steeds weer nieuwe mogelijkheden van fraude. Een technologie neutrale aanpak moet ervoor zorgen dat het rechtskader relevant en actueel blijft ook gelet op nieuwe technologische ontwikkelingen (toekomstbestendig dus). Dit zou er in de toekomst toe moeten

kst-35656-6
ISSN 0921 - 7371
's-Gravenhage 2021

leiden dat nieuwe technieken niet automatisch vragen om een wetswijziging, maar dat de gedragingen op zowel Europees als nationaal niveau al onder de vigerende wetgeving vallen. Ik zie deze benadering dus als een voordeel voor de aanpak van (nieuwe) criminele activiteiten.

Met betrekking tot het aanpalend beleid vragen de leden van de VVD-fractie in hoeverre de regering nauwer wil samenwerken met het bedrijfsleven om frauduleuze praktijken in kaart te brengen, hoe de gegevensuitwisseling tussen financiële instellingen en de overheid wordt vormgegeven en hoe financiële instellingen onderling gegevens kunnen uitwisselen. In reactie op deze vragen merk ik het volgende op. De politie en financiële instellingen werken samen in diverse samenwerkingsverbanden, waaronder de Electronic Crimes Taskforce (ECTF) (bancaire fraude) en het Landelijk Meldpunt Internetoplichting (LMIO) (online handelsfraude). In mijn brieven van 20 mei *(Kamerstukken II* 2019/20, 28 684, nr. 621) en 17 november jl. *(Kamerstukken II* 2019/20, 28 684, nr. 638) heb ik u uitgebreid geïnformeerd over de projecten die de banken en politie hebben ingericht om hun samenwerking te versterken. Op deze plaats wijs ik in het bijzonder de ECTF, een samenwerkingsverband tussen de politie, het OM, de Nederlandse grootbanken (ING, ABN/AMRO, Rabobank, Volksbank) en ICS cards. In de ECTF worden kennis, informatie en expertise samengebracht. Dit draagt bij aan betere analyses en een versterking van de informatiepositie. De samenwerking is zowel gericht op het voorbereiden van opsporingsonderzoeken naar fenomenen als fraude en phishing als op preventie en verstoring van dergelijke activiteiten. De ECTF is ondergebracht bij het Team High Tech Crime (THTC) van de politie waardoor snel geschakeld kan worden. De ECTF wordt in het door de Europese Commissie opgestelde impact assessment bij het destijds ingediende richtlijnvoorstel genoemd als een «best practice» in het kader van publiek-private samenwerking (zie SWD(2017)298, p. 52).

Bij de behandeling van de Wet gegevensverwerking door samenwerkingsverbanden heeft het lid Yesilgöz opnieuw aandacht gevraagd voor de positie van banken en hun wens om meer ruimte te krijgen om fraudeurs voor te zijn en voor internationale samenwerking op dat vlak. Ik heb aangegeven om de mogelijkheid voor de gegevensuitwisseling via LMIO en ECTF in het kader van die wet zorgvuldig te zullen onderzoeken *(Kamerstukken II* 2020/21, 35 447, nr. 20). Gegevensdeling tussen (nationale) financiële instellingen onderling moet thans voldoen aan de AVG en UAVG en is mogelijk met een vergunning van de Autoriteit Persoonsgegevens. Ook heb ik toegelicht *(Kamerstukken II* 2020/21, aanhangsel 438) dat banken ter voorkoming van fraude de IBAN-naam check ingevoerd. Bij deze check krijgen klanten een melding als de naam en het rekeningnummer die de klant invoert niet in overeenstemming zijn met de gegevens die bekend zijn bij de bank. Daarnaast werken de banken met verschillende fraudedetectiesystemen om frauduleuze transacties op te sporen en te onderzoeken. De monitoring vindt plaats op basis van vele indicatoren. In samenwerking met de politie wordt op basis van bepaalde modus operandi gekeken welke indicatoren gehanteerd kunnen worden om de fraudedetectiesystemen verder te verbeteren. Wanneer een mogelijk frauduleuze transactie gedetecteerd wordt door het fraudedetectiesysteem, wordt de transactie apart gezet en onderzocht door een medewerker van de bank, waarbij vrijwel altijd contact gezocht wordt met de klant. Met deze fraudedetectiesystemen kunnen banken dus tijdig fraude signaleren en klanten hiervoor waarschuwen. Door de grote aantallen overboekingen die dagelijks worden uitgevoerd is het ondoenlijk om ter controle een telefoontje te plegen naar elke klant.

In het kader van de gegevensuitwisseling en de bestrijding van witwassen en terrorismefinanciering merken de leden van de VVD-fractie op dat zij teleurgesteld zijn over het feit dat hierover nog geen wetsvoorstel naar de Tweede Kamer is gestuurd. In reactie hierop stel ik voorop ik met de leden van deze fractie meen dat effectieve gegevensuitwisseling cruciaal is voor de aanpak van witwassen en terrorismefinanciering. Het wetsvoorstel plan van aanpak witwassen, waaraan deze leden refereren, maakt onderdeel uit van het plan van aanpak witwassen *(Kamerstukken II* 2018/19, 31 477, nr. 41). Samen met mijn ambtgenoot van Financiën heb ik recent met uw Kamer overleg gevoerd over de voortgang van dit plan van aanpak, waarover uw Kamer periodiek is geïnformeerd *(Kamerstukken II* 2019/20, 31 477, nrs. 50, 51 en 53). In dat kader is aangegeven dat voornoemd wetvoorstel begin 2021 aan Uw Kamer wordt gezonden.

Tot slot vragen de leden van de VVD-fractie op welke manier de samenwerking met andere Europese landen om over en weer fraude met niet-contante betaalmiddelen aan te kunnen pakken momenteel is vormgegeven en welke plannen er zijn om deze fraudebestrijding centraal te faciliteren op Europees niveau. Ook willen deze leden weten welke rol hiervoor bij banken is belegd en welke rol hiervoor is weggelegd voor de bedrijven die niet-contante betaalmiddelen uitgeven of de platforms die deze producten verhandelen. Deze vragen beantwoord ik als volgt. Op Europees niveau wordt fraudebestrijding centraal gefaciliteerd door Europol. Europol heeft het analyse project Terminal opgezet ter ondersteuning van de honderden politie onderzoeken van EU lidstaten naar internationale fraude met niet-contante betaalmiddelen en online fraude. Op basis van de analyses kan er effectief worden gereageerd op nieuwe dreigingen en criminele netwerken. Dit gebeurt in samenwerking met de politie, de private sector en instanties, zoals de Europese Centrale Bank. Europol houdt zich op Europees niveau ook bezig met de bestrijding van fraude met niet-contante betaalmiddelen. Europol heeft ter bestrijding van financiële cybercrime, waaronder deze vormen van fraude, een alliantie gesloten met de European Banking Federation. Banken zijn op Europees niveau verenigd in deze European Banking Federation (EBF). De EBF heeft een samenwerkingsalliantie gesloten met Europol. Europol deelt regelmatig kennis met en initieert voorlichtingscampagnes in samenwerking met de EBF, in het bijzonder met de werkgroep cybersecurity and fraud van de EBF. De EMMA-campagne tegen geldezels is hiervan een voorbeeld.

De leden van de GroenLinks-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Tot mijn genoegen juichen deze leden het toe dat de strafrechtelijke bescherming wordt aangepast aan nieuwe betaalvormen en aan nieuwe vormen van misbruik. De vragen die deze leden nog hebben over (met name) de uitvoeringsaspecten beantwoord ik graag in paragraaf 4.

De leden van de SP-fractie hebben met interesse kennisgenomen van het wetsvoorstel. Deze leden vragen wat deze wetswijziging concreet verandert in de justitiële samenwerking met andere lidstaten. Ook vernemen zij graag in hoeverre andere lidstaten de richtlijn al in bestaande wetgeving hebben vastgelegd. Deze leden merken terecht op dat de Nederlandse wetgeving in belangrijke mate al aan de richtlijn voldoet. Onderhavige richtlijn vervangt een Kaderbesluit uit 2001 (Kaderbesluit 2001/413/JBZ). Voor zover gedragingen reeds vielen onder de bepalingen uit dat kaderbesluit, zouden deze dus ook reeds strafbaar moeten zijn in de verschillende lidstaten. In een aantal lidstaten is dit (nog) niet volledig gebeurd (zie de Evaluatie van het bestaande EU-beleid en wetgeving (annex 5 bij de hierna nog te bespreken impact assessment, p. 216). Daarnaast zijn er andere richtlijnen die zien op gedragingen die

kunnen samenhangen met online betaalfraude en die eveneens reeds door de lidstaten geïmplementeerd moeten zijn, zoals de Richtlijn aanvallen op informatiesystemen (Richtlijn 2013/40/EU).

Het richtlijnvoorstel over niet-contante betaalfraude (COM(2017) 489) werd destijds vergezeld door een impact assessment uitgevoerd door de Europese Commissie (SWD(2017)299). In dat impact assessment concludeert de Commissie onder andere (p. 20) dat bepaalde misdrijven die samenhangen met niet-contante betaalmiddelen niet effectief kunnen worden vervolgd omdat de desbetreffende gedragingen in lidstaten niet of verschillend strafbaar zijn gesteld. Dit betreft met name gedragingen betreffende elektronische betaalinstrumenten – die in het betaalverkeer een steeds belangrijkere rol krijgen en buiten de definitie van het Kaderbesluit uit 2001 vallen. Hetzelfde geldt volgens de Commissie voor voorbereidende handelingen, zoals «phishing», «skimming» en «carding». Verder constateert de Commissie (p. 21) dat hoewel een deel van deze gedragingen onder de hiervoor genoemde Richtlijn aanvallen op informatiesystemen valt, die richtlijn is gericht op bescherming van gegevensdragers. Dit biedt, aldus het rapport, niet per definitie volledige strafrechtelijke bescherming tegen online betaalfraude, die immers ook kan plaatsvinden zonder dat er bijvoorbeeld sprake is van computervredebreuk.

Ten aanzien van de onderlinge samenwerking met andere lidstaten geldt dat fraude met niet-contante betaalmiddelen een belangrijke grensoverschrijdende dimensie heeft die wordt versterkt door een steeds verdergaande digitalisering van het betaalverkeer. Dit betekent dat online betaalfraude door verdachten vanuit meerdere lidstaten kan worden gepleegd en dat er in meerdere lidstaten burgers, bedrijven en overheden slachtoffer kunnen worden. Daarom is het van belang dat tussen lidstaten kan worden samengewerkt om ook online betaalfraude aan te pakken. Voor deze samenwerking is het aangewezen dat gedragingen die samenhangen met deze vorm van fraude in alle lidstaten strafbaar zijn gesteld. Dit voorkomt dat bijvoorbeeld een vereiste van dubbele strafbaarheid in de weg staat aan het verlenen van rechtshulp en maakt het mogelijk dat lidstaten samenwerken in het kader van een opsporingsonderzoek naar (grootschalige) online betaalfraude. Een vergelijkbaar niveau van strafrechtelijke bescherming in alle lidstaten voorkomt ook «safe havens» binnen de Europese Unie, waarbij criminelen – straffeloos – vanuit een lidstaat waarin de gedragingen niet strafbaar zijn gesteld (online) strafbare feiten in een andere lidstaten zouden kunnen plegen. Verder zijn in de richtlijn enkele bepalingen opgenomen, specifiek gericht op de verbetering van de onderlinge samenwerking, waaronder de bepaling inzake informatie-uitwisseling (artikel 14 van de richtlijn).

De overige vragen van de leden van de SP-fractie, onder andere over de voorlichting van inwoners en ondernemers, de techniek neutrale formulering van de richtlijn, het herstel van een eerdere omissie en de financiële consequenties beantwoord ik in het navolgende.

De leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel en constateren met instemming dat de regering de adviezen van de Afdeling advisering van de Raad van State heeft verwerkt. Deze leden hebben aangegeven geen behoefte te hebben aan het stellen van nadere vragen.

De leden van de SGP-fractie hebben kennisgenomen van het voorstel te komen tot een implementatie van de richtlijn voor niet-contante betaalinstrumenten. Zij hebben hierover nog enkele vragen gesteld die in het navolgende worden beantwoord.

2. Hoofdlijnen richtlijn

Niet-contante betaalinstrumenten

Met betrekking tot het begrip «niet-contante betaalinstrumenten» vragen de leden van de VVD-fractie of alle gangbare fraudevormen, waaronder «spoofing» en «phishing», volledig onder het bereik van deze richtlijn vallen en of verhandelbare schulden als IOU's («I owe you») en obligaties ook onder deze definitie vallen. Voorts vragen voornoemde leden in hoeverre gebonden betaalproducten, zoals een OV-chipkaart, een boekenbon en beltegoeden onder de richtlijn vallen. Ik ga eerst in op de vraag of de genoemde «voorwerpen» onder de richtlijn vallen. Ik kan de leden bevestigen dat een OV-chipkaart, een boekenbon en beltegoed zijn aan te merken als een niet-contant betaalinstrument in de zin van het voorgestelde artikel 80septies Sr. Blijkens die definitiebepaling kan een niet-contant betaalinstrument onder andere een *beveiligd voorwerp* zijn waarvan gebruik wordt gemaakt voor het initiëren van een betaalopdracht. Dit is de «fysieke» variant van een niet-contant betaalmiddel. In de eerste plaats kan bij een «beveiligd voorwerp» worden gedacht aan een bankpas of creditcard, maar hieronder vallen ook een fysieke OV-chipkaart en een boekenbon. Een betaalopdracht is volgens artikel 1:1 van de Wet financieel toezicht (Wft) een «door een betaler of betalingsbegunstigde aan zijn betaaldienstverlener gegeven opdracht om een betalingstransactie uit te voeren». Uit datzelfde artikel van de Wft volgt dat een betalingstransactie een «door de betaler of de betalingsbegunstigde geïnitieerde handeling is waarbij geldmiddelen worden gedeponeerd, overgemaakt of opgenomen, ongeacht of er onderliggende verplichtingen tussen de betaler en de betalingsbegunstigde zijn» en dat geldmiddelen «chartaal geld, giraal geld of elektronisch geld» zijn. Elektronisch geld is geldswaarde die elektronisch of magnetisch is opgeslagen die onder meer een vordering op de uitgever vertegenwoordigt (denk hierbij aan beltegoed) of is uitgegeven in ruil voor ontvangen geld (ook hier kan gedacht worden aan beltegoed, maar dus ook de waarde die een boekenbon of OV-chipkaart vertegenwoordigt). Een boekenbon en een OV-chipkaart zijn ook voorbeelden van een waardekaart, zoals thans opgenomen in artikel 232 Sr. In het voorgestelde artikel 232 komen de termen betaalpas en waardekaart te vervallen. In de memorie van toelichting is ter onderbouwing hiervan opgenomen dat deze termen niet nodig zijn, omdat zij reeds vallen onder de term niet-contant betaalinstrument. Ook hieruit blijkt dat een boekenbon en een OV-chipkaart onder deze nieuwe definitie vallen.

Voor verhandelbare schulden als IOU's en obligaties geldt dat dit vormen van een schuldbewijs zijn. Een schuldbewijs vertegenwoordigt een belofte van de kredietnemer om op een bepaald tijdstip of bepaalde tijdstippen in de toekomst een of meerdere betalingen aan de kredietverstrekker te verrichten. In de zin van de Wet op het financieel toezicht zijn het daarmee effecten (artikel 1:1). Effecten zijn niet geschikt het voor het initiëren van een betaalopdracht als bedoeld in artikel 80septies Sr en daarmee vallen IUO's en obligaties niet onder de definitie van een niet-contant betaalinstrument in de zin van die bepaling. Hierbij merk ik wel op dat het frauderen met dit soort schuldbewijzen (bijvoorbeeld het vervalsen daarvan) weliswaar niet onder het bereik van de richtlijn valt, maar wel strafbaar is op grond van (de artikelen 225 en 326) van het Nederlandse Wetboek van Strafrecht.

De vraag van de leden van de VVD-fractie over «phishing» en «spoofing» beantwoord ik graag als volgt. «Phishing» is een methode die wordt gebruikt om waardevolle persoonlijke gegevens, zoals gebruikersnaam, wachtwoord en pincode te verkrijgen. In veel gevallen wordt daarvoor een

valse e-mail of tekstbericht verstuurd. De gegevens die hiermee worden verkregen, vallen onder de definitie van niet-contante betaalinstrument (de elektronische variant; afgeschermde gegevens geschikt voor het initiëren van een betaalopdracht). Bij «spoofing» wordt door de verdachte(n) een truc gebruikt om (tijdelijk) een andere identiteit aan te nemen. Het slachtoffer ontvangt dan bijvoorbeeld een e-mail van een bestaand e-mailadres van een bank, maar de mail is niet echt verzonden door die bank. Ook bestaat er website-spoofing waarbij het slachtoffer via een link op een website terecht komt, die echt lijkt maar dat niet is. Met spoofing wordt eveneens geprobeerd gegevens te verkrijgen waarmee betaalopdrachten kunnen worden geïnitieerd. Op grond van artikel 5, onderdeel a, van de richtlijn dient ook de onrechtmatige verkrijging van elektronische betaalinstrumenten strafbaar te worden gesteld door de lidstaten. Phishing en spoofing vallen daarmee onder het bereik van de richtlijn. In Nederland zijn phishing en spoofing al strafbaar op grond van artikel 326 Sr (oplichting).

Gedragingen

De leden van de SGP-fractie verwezen naar het vereiste dat de verdachte moet hebben gehandeld met een frauduleus oogmerk. Dit is in de richtlijn tot uitdrukking gebracht met de woorden «frauduleuze», «met het oog op het frauduleus gebruik daarvan», «met het oogmerk een wederrechtelijke voordeel voor de dader of een derde te behalen» en «met het oogmerk deze middelen daarvoor te gebruiken». Zij vroegen hoe dit bestanddeel, althans zo begrijp ik hun vraag, bewezen kan worden als het gaat om een gedraging die online wordt gepleegd. Graag beantwoord ik deze vraag als volgt. Blijkens overweging 14 bij de richtlijn mag het vereiste oogmerk worden afgeleid uit objectieve, feitelijke omstandigheden. In de Nederlandse strafwet is het frauduleuze oogmerk in de diverse relevante wettelijke bepalingen tot uitdrukking gebracht met de woorden «met het oogmerk zichzelf of een ander wederrechtelijk te bevoordelen» (hierna: het oogmerk van wederrechtelijke bevoordeling). Het oogmerk van wederrechtelijke bevoordeling komt op dit moment al op verschillende plekken in het Wetboek van Strafrecht voor, waaronder bij verschillende delicten die ook online gepleegd (kunnen) worden (zie o.a. de artikelen 138ab en 326 Sr). Hoewel een oogmerk in de Nederlandse rechtspraak als een bijzondere vorm van opzet wordt beschouwd, betekent dit niet dat oogmerk gelijkgesteld kan worden aan de (diepste, innerlijke) bedoeling van de verdachte. Bij het bewijs van een oogmerk kan bovendien worden gebruikgemaakt van een objectiverende bewijsvoering. Dit geldt ook ten aanzien van het bewijs van het oogmerk van wederrechtelijke bevoordeling, dat in de rechtspraak ruim wordt uitgelegd. Dat sprake is van het oogmerk van wederrechtelijke bevoordeling wordt in voorkomende gevallen in de rechtspraak afgeleid uit omstandigheid dat de verrichte gedraging wederrechtelijk is en is gericht op het verkrijgen van voordeel. Vgl. *T&C Sr*, artikel 317, aant. 6 en artikel 326, aant. 7; NLR, art. 326, aant. 6, HR 5 januari 1982, *NJ* 1982/232 *(Gevangenisvoedsel II*); HR 16 oktober 1991/153, *NJ* 1991/153; HR 10 januari 2017, ECLI:NL:HR:2017:28, *NJ* 2017/162, r.o. 3.3. In de (feiten)rechtspraak zijn ook diverse voorbeelden te vinden van zaken waarin sprake was van online betaalfraude en waarin uit de gepleegde gedragingen werd afgeleid dat sprake was van een oogmerk van wederrechtelijke bevoordeling. Dit oogmerk werd bijvoorbeeld afgeleid uit de omstandigheid dat phishingmails of sms-berichten werden verstuurd om zo aan inlogcodes voor internetbankkieren, pincodes, bankpassen of rekeningnummers te komen of om slachtoffers te bewegen geld over te maken (vgl. Rb. Amsterdam 24 januari 2017, ECLI:NL:RBAMS:2017:382; Rb. Noord Holland 28 februari 2019, ECLI:NL:RBNHO:2019:1572; Rb. Den Haag 29 juni 2020, ECLI:NL:RBDHA:2020:5798), de omstandigheid dat de

verdachten zich onrechtmatig toegang hadden verschaft tot een zelfservicewebsite en daar bankrekeningnummers van personeelsleden hadden gewijzigd in bankrekeningnummers van derden of waren binnengedrongen op webportals van creditcardhouders om vervolgens bestellingen te plaatsen en geld over te maken (Hof Den Haag 26 november 2019, ECLI:NL:GHDHA:2019:3148; Rb. Amsterdam 25 maart 2020; ECLI:NL:RBAMS:2020:1961) en de omstandigheid dat de verdachten de slachtoffers omleidden naar een valse website om hen (de verdachten) zo toegang te verschaffen tot het mobiel bankieren van de slachtoffers of om hen geld over te laten maken (vgl. Rb. Zeeland-West-Brabant 17 mei 2019, ECLI:NL:RBZWB:2019:2195; Rb. Den Haag 22 december 2017, ECLI:NL:RBDHA:2017:15273).

3. Hoofdlijnen wetsvoorstel

De leden van de SP-fractie vragen zich, onder verwijzing naar overweging 11 van de richtlijn, af of factuur- en CEO-fraude strafbaar wordt gesteld in de gehele Europese Unie en of deze vormen van fraude met deze richtlijn definitief de aandacht krijgen in de gehele EU die zij verdienen. Daarnaast vragen deze leden om toe te lichten hoe de Nederlandse autoriteiten beter worden uitgerust om deze vormen van fraude te bestrijden nu andere lidstaten deze vormen van fraude ook strafbaar gaan stellen. Graag beantwoord ik deze vragen in onderlinge samenhang als volgt. In overweging 11 van de richtlijn is opgenomen dat het verzenden van valse facturen om betalingslegitimatiegegevens te verkrijgen, moet worden beschouwd als een poging tot wederrechtelijke toe-eigening binnen de werkingssfeer van de richtlijn. Deze beperking tot betalingslegitimatiegegevens is aangebracht in verband met de reikwijdte van de richtlijn, die immers ziet op niet-contante betaalinstrumenten. Deze overweging – waarvan het belang ook door de regering ten zeerste worden erkend – is een gevolg van amendementen ingediend door het Europees Parlementslid De Jong (SP) bij de richtlijn. De overwegingen spelen een belangrijke rol bij de interpretatie van richtlijnen. Dit betekent in dit geval dat lidstaten gehouden zijn om ervoor te zorgen dat voornoemde gedraging valt binnen de reikwijdte van hun strafwetgeving. Zoals in paragraaf 1 van deze nota, naar aanleiding van een vraag van deze leden reeds is opgenomen, draagt een vergelijkbare strafrechtelijke bescherming bij aan de verbetering van de samenwerking binnen de EU. Dat zal ook gelden ten aanzien van de hier genoemde vorm van fraude, nu alle lidstaten gehouden zijn om ervoor te zorgen dat deze gedraging onder de reikwijdte van hun strafwetgeving valt. Met deze richtlijn zal het voor de Nederlandse autoriteiten, indien er sprake is van een grensoverschrijdende dimensie, dus makkelijker zijn om samen te werken met andere lidstaten om de verdachte op te sporen en te vervolgen.

In de inleiding van deze nota is bij de beantwoording van enkele vragen van de leden van de VVD-fractie al ingegaan op de techniek-neutrale formulering van de richtlijn. De leden van de SP-fractie merken terecht op dat dit tot meer abstracte formuleringen in de tekst leidt en vragen wat de keerzijde is van de keuze om de richtlijn techniekneutraal te formuleren. In dit kader vragen zij voorts waarom de bestaande artikelen in het Wetboek van Strafrecht die met dit voorstel gewijzigd worden nog niet techniekneutraal zijn en in hoeverre andere artikelen uit het wetboek techniekneutraal zijn geformuleerd. Voor wat betreft mijn appreciatie van de enigszins abstracte formuleringen die in deze richtlijn zijn gebruikt, verwijs ik deze leden graag naar mijn positief getoonzette reactie op de vragen van de leden van de VVD-fractie hierover in de inleiding van deze nota. Wat een keerzijde van abstracte en techniek neutrale formuleringen kan zijn, zo beantwoord ik de vraag daarover van deze leden, is dat er een gevaar kan ontstaan van een te onbepaald begrippenapparaat waardoor regelgeving

uit een oogpunt van rechtszekerheid niet meer voldoet aan eisen van bepaaldheid en begrijpelijkheid. Ik meen evenwel dat de Europese wetgever met de in deze richtlijn opgenomen teksten wat betreft woordkeus een juiste balans heeft gevonden tussen het gebruik van enerzijds terminologie die in voldoende mate in afgrenzing voorziet en anderzijds concepten met een zekere van mate van abstractie die aan de regeling een duurzaam karakter geven. In reactie op de vraag van deze leden over het Wetboek van Strafrecht stel ik graag voorop dat ook dit wetboek zich voornamelijk kenmerkt door strafbaarstellingen die eenvoudig, helder en in betrekkelijk algemene bewoordingen zijn geformuleerd. Ook de oudere delictsomschrijvingen kunnen hierdoor nog na lange tijd dikwijls zonder problemen worden toegepast. De rechter is in staat gebleken de begrippen in het wetboek te interpreteren en waar nodig aan te passen aan de zich veranderende maatschappij. Dit is in belangrijke mate ook te danken aan het veelal techniek neutrale karakter van de begrippen die in het wetboek worden gebezigd. Slechts op specifieke terreinen komt zo nu en dan naar boven dat bepaalde delicts-omschrijvingen of daarin opgenomen bestanddelen bijstelling behoeven om ook hun werking zeker te stellen en duidelijk te maken in verband met technologische ontwikkelingen, zoals de introductie van het elektronisch bankieren en meer in het algemeen de komst van het internet. Illustratief is in dit verband de introductie van de delicten als computervredebreuk (artikel 138ab Sr) en de vernieling van computergegevens (artikel 350a Sr). Tegen deze meer in den brede geschetste achtergrond – waaraan ook betekenis is gegeven in de memorie van toelichting bij dit wetsvoorstel – moeten ook de techniek-neutrale aanpassingen worden beschouwd die het gevolg zijn van de implementatie van de richtlijn. Het betreft dan met name de omschrijving van het begrip niet-contant betaalinstrument in artikel 80septies Sr en de verruiming van artikel 232 Sr waardoor ook het gebruikmaken van valse of vervalste elektronische betaalinstrumenten zelfstandig strafbaar wordt.

Tot slot vragen de leden van de SP-fractie naar de verplichte voorlichting van inwoners en ondernemers over de gevaren van de in de richtlijn genoemde vormen van fraude. Zij vragen of het klopt dat de regering niet overgaat tot aanvullende of actieve voorlichting van inwoners en ondernemers en of de regering deze keuze kan toelichten, met name in het licht van de explosieve toename van cybercrime die in Nederland is geconstateerd ten tijde van de coronacrisis. In antwoord op deze vraag kan ik aangeven dat mijn ministerie zich tezamen met het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), het Ministerie van Economische Zaken en Klimaat (EZK), publieke- en private partijen actief inzet op preventie en bewustwording van gedigitaliseerde criminaliteit en cybercrime. Dit vindt plaats door middel van algemene voorlichting en campagnes gericht op specifieke fenomenen en doelgroepen. Het is van groot belang dat de preventieactiviteiten aansluiten op de actualiteit en ook de kwetsbare groepen weet te bereiken. De kwetsbare groepen zijn jongeren, senioren, laaggeletterde en de MKB-ondernemers. Hoe specifieker de communicatie richting de preventiedoelgroep is, des te effectiever de preventie. Concrete voorbeelden zijn onder meer het convenant »eerst checken, dan klikken». Dit convenant met publieke en private partijen is vernieuwd en met drie jaar verlengd. Deze voortzetting richt zich op de preventie van cybercrime. Zo zal de campagne «Senioren en Veiligheid» ook dit jaar worden herhaald. In deze campagne worden senioren gewaarschuwd voor hulpvraagfraude via WhatsApp, phishing en spoofing. Stichting Halt heeft in opdracht van het Centrum van Criminaliteitspreventie en Veiligheid en mijn ministerie een voorlichtingsmodule «online fraude en cybercrime» voor het voortgezet onderwijs ontwikkeld, die deze maand landelijk beschikbaar is. In oktober 2020 is de City Deal Lokale weerbaarheid Cybercrime ondertekend, een samenwerkings-

verband tussen de Ministeries van Justitie en Veiligheid, BZK en EZK/Digital Trust Center (DTC) met regionale en lokale partners. Binnen de City Deal lopen achttien projecten van gemeenten, regionale samenwerkingsverbanden Veiligheid en PVO's gericht op het versterken van de weerbaarheid van burgers (jongeren, laaggeletterden en senioren) en het MKB. De projecten zijn gericht op handelingsperspectief voor gemeenten om de cyberweerbaarheid van burgers en bedrijven te vergroten en lopen tot medio 2021.

Ook EZK zet zich in om online veiligheid voor consumenten en ondernemer te vergroten. Dit gebeurt deels middels de bewustwordingscampagne «Doe je updates» en met de publiek-private website www.veiliginternetten.nl. Om bedrijven verder te helpen hun weerbaarheid te verhogen is door EZK in 2018 het DTC opgericht. De ondersteuning van het DTC kan gaan van awarenessactiviteiten en het beschikbaar stellen van tools zoals de cybersecurityscan en handelingsperspectieven (te beginnen met de 5 basisprincipes) tot het geven van concrete dreigingsinformatie en adviezen. Het DTC stimuleert tevens de samenwerking tussen de bedrijven zodat bedrijven elkaar kunnen helpen de weerbaarheid te vergroten (er zijn momenteel 31 samenwerkingsverbanden). Om alle verschillende initiatieven op het terrein van cybersecurity inzichtelijk te maken voor de bedrijven heeft het DTC woensdag 9 december jl. na intensieve samenwerking met het CIO Platform de «Cybersecurity Wegwijzer» gelanceerd. Ik heb ook de toezegging gedaan om te onderzoeken hoe een «cyberweerbericht» georganiseerd kan worden, waarin actuele dreigingsinformatie of informatie over modi operandi met burgers en bedrijven gedeeld kan worden *(Kamerstukken II* 2020/21, 28 684 nr. 645).

4. Inhoud richtlijn en wijze van implementatie

Artikel 5

De leden van de SGP-fractie constateren dat het hacken van een digitale sleutel om een virtuele wallet te openen voldoende kan zijn om een persoon (onder druk) te vragen elektronische valuta te verplaatsen naar de virtuele wallet van de hacker. In dit kader vragen deze leden of de regering kan aangeven of het achterhalen/hacken van een digitale sleutel tot een virtuele wallet voldoende is voor strafbaarstelling onder artikel 5 van de richtlijn. In antwoord op deze vraag verduidelijk ik graag dat artikel 5, onderdeel a, van de richtlijn verplicht tot strafbaarstelling van de wederrechtelijke verkrijging van elektronische betaalinstrumenten. Daarbij is bepaald dat deze gedraging in ieder geval strafbaar moet zijn gesteld indien bij die verkrijging een van de in de artikelen 3 tot en met 6 van de eerder in deze nota al genoemde Richtlijn aanvallen op informatiesystemen is gepleegd. Deze richtlijnbepalingen zien onder andere op «hacken». Onderhavige richtlijn (de richtlijn fraude met niet-contante betaalmiddelen) heeft eveneens betrekking op digitale sleutels om toegang te verkrijgen tot virtuele wallets waarin virtuele valuta kunnen worden opgeslagen. Zij moeten worden beschouwd als een niet-contant betaalinstrument, zo kan worden afgeleid uit artikel 2, onder a en c, in combinatie met overweging 10 van de richtlijn. Het hacken van een digitale sleutel waarmee toegang kan worden gekregen tot een wallet valt daarmee onder de reikwijdte van (artikel 5 van) de richtlijn. Nederland heeft deze bepaling ruim geïmplementeerd in die zin dat niet alleen in de gevallen waarin de computerdelicten genoemd in de artikelen 3 tot en met 6 van de Richtlijn aanvallen op informatiesystemen zijn gepleegd, sprake is van een strafbare gedraging, maar ook wanneer de betreffende gegevens op een andere onrechtmatige wijze – door diefstal, afpersing, verduistering of oplichting – zijn verkregen.

Artikel 6

De leden van de SGP-fractie vragen, in het kader van artikel 6 van de richtlijn, of de persoon die gegevens doorgeeft, althans zo begrijp ik hen, ook naar Nederlands recht over een frauduleus oogmerk moet beschikken. De term «doorgeeft» is toegevoegd aan artikel 138c Sr, omdat binnen deze bepaling al verschillende andere gedragingen vallen die daarmee samenhangen. De gedraging past daarmee beter in die bepaling dan in bijvoorbeeld de artikelen 350a en 350c Sr, zoals in een eerder concept van dit wetsvoorstel voorgesteld. Het huidige artikel 138c Sr bevat niet het vereiste dat de verdachte ook het oogmerk van wederrechtelijke bevoordeling heeft gehad. Daarmee wordt dit naar Nederlands recht niet vereist. Wel moet de verdachte de gegevens opzettelijk en wederrechtelijk doorgeven. Als het oogmerk van wederrechtelijke bevoordeling bewezen kan worden, geldt op grond van het voorgestelde artikel 138c, derde lid, Sr een hoger strafmaximum. Met het derde lid wordt uitvoering gegeven aan artikel 9, vierde lid, van de richtlijn, op grond waarvan lidstaten verplicht zijn op het in artikel 6 van de richtlijn bedoelde strafbare feit (dus inclusief het oogmerk) een straf te stellen van ten minste drie jaar.

Artikel 9

Artikel 9 van de richtlijn ziet op de sancties die op de in de richtlijn genoemde strafbare feiten moeten worden gesteld. De leden van de SGP-fractie constateren dat deze bepaling van lidstaten vraagt om eenduidigheid wanneer als sanctie op de strafbare feiten een maximale straf staat die minimaal een bepaalde periode bedraagt. Dit kan volgens deze leden tot een verdeeld strafklimaat in Europa leiden voor hetzelfde strafbare feit. Zo kan het lonend zijn voor fraudeurs om in de lidstaat met de laagste strafmaat te gaan opereren, aldus de leden van de SGP-fractie die daarom vragen of de regering kan aangeven of zij deze verdeeldheid in strafklimaat in lidstaten ook ziet en hoe zij bovengenoemde situatie wil voorkomen. In het algemeen is het zo dat de verschillende strafstelsels in de Europese Unie historisch gegroeid zijn binnen de nationale staten en zich hebben ontwikkeld in het kader van de specifieke normen en waarden die in de desbetreffende lidstaten belangrijk werden geacht; zij hebben hun eigen innerlijke coherentie en consistentie. Sinds de Europese Unie in de jaren negentig van de vorige eeuw, in de Verdragen van Maastricht en Amsterdam, een taak op het terrein van het strafrecht heeft gekregen, zet zij zich evenwel in om ten aanzien van belangrijke grensoverschrijdende criminaliteitsvormen op het gebied van strafbaarstellingen en strafmaxima een grotere onderlinge afstemming in de strafwetgeving van alle lidstaten te realiseren. Dit met als doel om daarmee samenhangende beletselen in het kader van de internationale rechtshulp weg te nemen, maar ook – waarop deze leden hebben geattendeerd – om een gelijkwaardig niveau van strafrechtelijke bescherming in de lidstaten tot stand te brengen waardoor zogenaamde «safe havens» zoveel mogelijk worden voorkomen. Daarbij wordt bij de totstandbrenging van bindende Europese besluiten al sinds langere tijd gebruik gemaakt van de ook in deze richtlijn gehanteerde wetgevingstechniek die de lidstaten in elk geval verplicht te voorzien in een maximumstraf van (minimaal) een bepaalde hoogte. Naar de mening van de regering moet juist deze techniek als een doeltreffend instrument worden beschouwd om de verdeeldheid in het strafklimaat in de lidstaten, voor zover die tot uitdrukking komt in de nationaal wettelijke strafmaxima, voor een belangrijk deel ongedaan te maken. Deze minimale maximumstraf geeft blijk van consensus op het niveau van de Europese Unie over de ernst en strafwaardigheid van een bepaald delict in zijn zwaarste verschijningsvorm en garandeert de verplichting dat binnen de nationale rechtsordes deze sanctie voor de strafrechtelijke autoriteiten bij

de vervolging en bestraffing van het desbetreffende delict een belangrijk oriëntatiepunt vormt doordat ten minste die strafpositie als wettelijk strafmaximum in de wet moet zijn verankerd. In dat licht is de regering daarom ook niet beducht voor het effect waarvoor deze leden vreesden, in die zin dat juist de hoogte van de minimale maximumstraf fraudeurs uitnodigt die feiten te begaan in de lidstaten waar het strafmaximum daarop is afgestemd. Daarbij komt overigens dat naast de strafhoogte, ook bijvoorbeeld de pakkans, van groot belang is. Deze richtlijn draagt bij aan het vergroten van die pakkans, niet alleen doordat de in de richtlijn opgenomen gedragingen in alle lidstaten strafbaar worden gesteld – hetgeen bijdraagt aan (betere) onderlinge samenwerking bij de opsporing en vervolging –, maar ook door de specifieke voorschriften die in de richtlijn zijn opgenomen over rechtsmacht, de uitwisseling van informatie (met financiële instellingen en met andere lidstaten) en de beschikbaarheid van meldkanalen voor slachtoffers van deze vorm van fraude.

In het kader van de sancties vragen deze leden ook of de regering kan aangeven of het uitvoeren, handhaven en berechten van de strafbare feiten in deze richtlijn in ieder lidstaat dezelfde prioriteit krijgt. Over de wijze waarop iedere lidstaat prioriteit geeft aan de handhaving en berechting van de strafbare feiten waarop deze richtlijn ziet, heeft de regering op dit moment geen zicht. Waar in het verleden de uitvoering en toepassing van EU-kaderbesluiten niet werkelijk kon worden afgedwongen, is hier echter door het Verdrag van Lissabon verandering in gekomen. Het Europees strafrecht, waarvan deze richtlijn onderdeel uitmaakt, vormt een volwaardig onderdeel van de Europese rechtsorde, op de totstandkoming uitvoering waarvan de Europese Commissie stevig toeziet. Zo nodig kan zij die uitvoering ook met de haar ter beschikking staande instrumenten, zoals het initiëren van een inbreukprocedure bij het Hof van Justitie, afdwingen. Om deze taak van de Commissie adequaat te ondersteunen bevat de onderhavige richtlijn in artikel 18 tamelijk gedetailleerde jaarlijkse verplichtingen voor de lidstaten tot informatieverschaffing over het aantal geregistreerde strafbare feiten en het aantal personen dat voor de in de richtlijn bedoelde strafbare feiten is vervolgd en veroordeeld, opdat de Commissie een goed beeld krijgt van de wijze waarop de lidstaten uitvoering geven aan de richtlijn. De Commissie zelf weet zich ingevolge hetzelfde artikel verplicht tot de vaststelling van een programma voor de monitoring van de uitkomsten, resultaten en effecten van de richtlijn. Bovendien is zij op grond van artikel 21 van de richtlijn gehouden tot een beoordeling van de naleving van de implementatieverplichtingen van de lidstaten en de verslaglegging daarover in 2023 aan het Europees Parlement alsmede tot het uitvoeren van een evaluatie in 2026 van de bredere consequenties van de richtlijn waar het gaat om de bestrijding van fraude met en vervalsing van niet-contante betaalmiddelen. Het is dit samenstel van informatieverplichtingen, toezichthoudende en handhavende bevoegdheden van de Commissie alsmede de publieke verantwoording over de eigen implementatieverrichtingen dat er naar het oordeel van de regering voor zal zorgen dat aan de handhaving van de wetgeving ter uitvoering van de richtlijn in iedere lidstaat de gewenste aandacht en prioriteit zullen worden gegeven.

Tot slot wijzen de leden van de SGP-fractie op het tweede lid van artikel 9 van de richtlijn. Uit die bepaling volgt dat lidstaten minimaal bepaalde straffen op de in de richtlijn in de artikelen 3 tot en met 6 opgenomen strafbare feiten moeten stellen. Deze leden constateren dat daar waar naar aanleiding van artikel 9 de straffen worden verhoogd, steeds de minimale maximumstraf is gekozen. Zij vroegen om een toelichting hierop. In het Nederlandse Wetboek van Strafrecht geldt dat door middel van de gekozen strafmaxima de ernst van de verschillende strafbare feiten in

onderlinge afstemming tot uitdrukking wordt gebracht. Bij de implementatie van een richtlijn moet daarom rekening worden gehouden met deze onderlinge verhouding tussen de verschillende strafmaten.

Ten aanzien van het overgrote deel van Nederlandse strafbaarstellingen waarmee de richtlijnbepalingen worden geïmplementeerd, geldt dat die reeds worden bedreigd met de vereiste minimale maximumstraf opgenomen in artikel 9 van de richtlijn of met een hogere straf. Indien van dit laatste sprake is, is daarin uiteraard geen wijziging gebracht. Ten aanzien van twee bepalingen – de artikelen 138b en 138c Sr – geldt dat de daarin opgenomen strafmaxima nog niet in overeenstemming zijn met artikel 9, tweede en vierde lid, van de richtlijn. Om die reden wordt voorgesteld de strafmaten voor die bepalingen te verhogen (artikel I, onderdelen B en C, van het wetsvoorstel). Overeenkomstig artikel 9, vierde lid, (jo. artikel 6) van de richtlijn zal op grond van het voorgestelde artikel 138b, tweede lid, Sr (computervredebreuk) een strafmaximum van drie jaar gelden (in plaats van de twee jaar voor het «basisdelict»; zie artikel 138b, eerste lid, Sr). Daarnaast wordt de maximale gevangenisstraf die is gesteld op artikel 138c Sr – ter implementatie van artikel 9, tweede lid, van de richtlijn – verhoogd van één naar twee jaar indien de doorgegeven of overgenomen gegevens een niet-contant betaalinstrument betreffen (het voorgestelde artikel 138c, tweede lid, Sr) en – ter implementatie van artikel 9, vierde lid, van de richtlijn – naar drie jaar indien het feit is gepleegd met het oogmerk van wederrechtelijke bevoordeling (het voorgestelde artikel 138c, derde lid, Sr). Met deze aanpassingen is sprake van een behoorlijke verhoging ten opzichte van het basisdelict. In het geval van artikel 138c Sr is zelfs sprake van een verdriedubbeling van de straf. De gekozen strafmaten zijn ook in lijn met de strafbedreiging die geldt voor andere computerdelicten (die zijn gepleegd onder strafverzwarende omstandigheden, zoals de inzet van een botnet) en andere strafbare feiten gericht op het opnemen of overnemen van gegevens.

Gevraagd naar wat de strafmaatverhogingen betekenen voor de praktijk, antwoord ik dat van de (behoorlijke) verhoging van het wettelijk strafmaximum een signaal van de wetgever uitgaat dat het desbetreffende strafbare feit (onder de genoemde strafverzwarende omstandigheden) als ernstiger en strafwaardiger moet worden beschouwd. Hoewel het openbaar ministerie en de rechter vrijheid toekomen bij het bepalen van de strafeis en de straftoemeting, mag verwacht worden dat zij bij het bepalen van de strafeis of strafmaat rekening zullen houden met dit signaal van de wetgever.

Artikel 14

De leden van de GroenLinks-fractie stellen enkele vragen over het Landelijk Internationaal Rechtshulpcentrum (LIRC), dat door Nederland wordt aangewezen als operationeel nationaal contactpunt. Zo vragen deze leden hoe de regering het praktische functioneren van dit centrum voor zich ziet en in hoeverre specialisatie plaatsvindt, gezien het vaak zeer gecompliceerde en hoogtechnologische karakter van deze criminaliteitsvormen. En meer in het bijzonder hoe de regering de samenwerking voor zich ziet met binnen- en buitenlandse financiële opsporingsdiensten en private dienstverleners inzake de signalering, opsporing en vervolging van (grensoverschrijdende) fraude met niet-contante betaalmiddelen. Ook vragen deze leden hoeveel fte bij het LIRC zal worden vrijgemaakt voor de bestrijding van misbruik van niet-contante betaalmiddelen. Deze vragen beantwoord ik als volgt. De richtlijn verplicht de lidstaten ertoe met het oog op informatie-uitwisseling over de feiten die strafbaar zijn gesteld in de richtlijn te beschikken over een operationeel nationaal contactpunt dat vierentwintig uur per dag, zeven dagen per week bereikbaar is (hierna:

24/7-contactpunt). In Nederland zijn het Landelijk Internationaal Rechtshulpcentrum (LIRC) en de elf regionale Internationale Rechtshulpcentra (IRC's) het internationale loket voor buitenlandse autoriteiten. Het LIRC en de IRC's vormen samen de Rechtshulpvoorziening Nederland. Het LIRC beheert vijf kanalen waarlangs de internationale informatie-uitwisseling plaats vindt en is 24/7 bereikbaar. Tenzij er andere afspraken zijn gemaakt, komen rechtshulpverzoeken binnen bij het LIRC en daar wordt beoordeeld via welk informatiekanaal het verzoek wordt uitgezet en welk onderdeel het verzoek gaat uitvoeren. Het team SIRENE van het LIRC neemt buiten kantooruren voor urgente verzoeken tot internationale samenwerking de taken over van de overige kanalen. Eenvoudige rechtshulpverzoeken handelen de (L)IRC's zoveel mogelijk zelf af. Complexere rechtshulpverzoeken worden via de (L)IRC's door generieke of thematisch meer specialistische rechercheteams (bijvoorbeeld THTC) in behandeling genomen. Gelet op bovenstaande is het LIRC de aangewezen instantie om als operationeel nationaal contactpunt te fungeren. Het LIRC heeft een generieke taak. Er wordt geen capaciteit gelabeld voor specifieke criminaliteitsvormen. Bij het LIRC is specifieke kennis aanwezig voor het verwerken en doorzetten van cyber gerelateerde rechtshulp. De verwachting is dat deze richtlijn niet zal leiden tot een wezenlijke wijziging van het totale van volume rechtshulpverzoeken. Ik antwoord op de vraag van deze leden over de samenwerking met buitenlandse opsporingsdiensten en private dienstverleners dat in opsporingsonderzoeken verzoeken om informatie van private dienstverleners verlopen via rechtshulpverzoeken tussen de opsporingsdiensten van de verschillende lidstaten. Ook hierin heeft de Rechshulpvoorziening Nederland een belangrijke rol, zowel voor inkomende als uitgaande verzoeken van rechtshulp.

Artikel 15

Artikel 15 van de richtlijn gaat over het melden van misdrijven via passende meldkanalen. De leden van de GroenLinks-fractie vragen de regering of met de huidige meldkanalen wel voldoende urgentie wordt gegeven aan de in omvang en complexiteit toenemende online financiële criminaliteit. Deze leden wijzen op de omvang van deze vormen van fraude en vragen de regering of het afdoende is om te volstaan met de huidige servicelijnen, waarvan het volgens de GroenLinks-fractie onduidelijk is hoe snel politie en justitie in actie komen. Deze leden vragen of de regering bereid is te voorzien in een toegankelijke aangifteprocedure, die in voorkomende gevallen kan leiden tot snelle interventies om het buiten bereik raken van vermogensbestanddelen te voorkomen. Ik antwoord hierop dat het van belang is dat slachtoffers van deze vormen van fraude snel ergens terecht kunnen en worden geholpen. Het snel melden van online van fraude is van belang, ook omdat geld snel doorgesluisd kan worden. Omdat hiervoor soms enkele muisklikken genoeg zijn, is het lang niet altijd mogelijk om geld dat wordt doorgesluisd te onderscheppen. Dat kan anders zijn als de opsporingsdiensten en banken tijdig zicht hebben op criminele organisaties en bankrekeningen die door hen of geldezels gebruikt worden. Zoals eerder in deze nota aangegeven wordt om die reden ingezet op de versterking van de samenwerking tussen banken en opsporingsdiensten. Een belangrijke stap daarbij is dat per 10 september 2020 de Wet en het Besluit verwijzingsportaal bankgegevens in werking zijn getreden. Het Verwijzingsportaal bankgegevens maakt het mogelijk dat geautomatiseerd binnen 30 seconden identificerende gegevens van banken en andere betaaldienstverleners kunnen worden verkregen ten behoeve van opsporingsonderzoeken. Zo kan de politie sneller en beter financieel onderzoek doen naar mogelijke fraudeurs. Het vorderen van saldo en transactiegegevens is een volgende stap bij financieel onderzoeken omdat het wenselijk is ook dit

proces te versnellen wordt samen met de aangesloten diensten en de banken gewerkt aan het automatiseren van dit proces.

Daarnaast spelen ook (andere) meldkanalen bij de politie een rol. Ook dan is van belang dat een de informatie snel op de juiste plek komt. Het is inmiddels mogelijk om online aangifte te doen van bepaalde vormen van internetfraude, zoals helpdeskfraude, aan- en verkoopfraude en Whatsapp-fraude. Hierdoor komt de aangifte direct bij de juiste specialistische afdeling terecht. Meldingen van mensen die aangifte willen doen op het politiebureau en telefonisch contact leggen met de politie of naar het bureau komen, zijn voor deze specialistische teams opvraagbaar. De politie hecht bijzonder aan het in verbinding staan met de burger, zowel fysiek als digitaal om haar politietaak goed uit te voeren. De omnichannelstrategie van politie is er op gericht dat bestaande kanalen voor burgercontact – zoals de internetaangifte – worden geactualiseerd om beter te kunnen voldoen aan de ontwikkelingen in de maatschappij. Ook worden er nieuwe kanalen ontwikkeld. Anderzijds worden de kanalen stap voor stap (beter) op elkaar afgestemd. Hierbij worden burgers betrokken («costumer journey») om er zodoende voor te zorgen dat aanpak voldoet aan de wensen en verwachtingen die burgers hebben.

De leden van de SGP-fractie constateren in het kader van dit artikel dat er veel samenwerkende organisaties zijn ter bestrijding van de in de richtlijn genoemde strafbare feiten. Deze leden vragen de regering wie hierbij de leiding heeft en of deze organisatie voldoende capaciteit heeft om de fraude adequaat en effectief te bestrijden. Het opsporen van strafbare feiten vindt plaats onder het gezag van het openbaar ministerie. Voor de inzet van het strafrecht is bepalend of er voldoende aanknopingspunten zijn. Uiteindelijk bepaalt het bevoegd gezag de prioriteit in de opsporing. Ook deze specifieke vorm van fraude moet worden gewogen binnen de totale opgave en inzet van het strafrecht. Dat betekent dat er nadere keuzes moeten worden gemaakt, waarbij rekening wordt gehouden met criteria zoals de maatschappelijke schade; recidive en impact op de samenleving.

Artikel 16

Artikel 16 van de richtlijn gaat over de bijstand en ondersteuning aan slachtoffers. De leden van de VVD-fractie zijn ingenomen met de nadrukkelijke aandacht die de richtlijn besteedt aan de hulp aan slachtoffers. Gelet op de klachten die deze leden echter hebben gehoord van mensen die aangifte wilden doen maar niet door de politie werden geholpen, vragen zij hoe zeker wordt gesteld dat slachtoffers van dit soort fraude te allen tijde aangifte kunnen doen. Als de aangifte niet wordt opgenomen willen deze leden weten waar burgers dan terecht kunnen en welke maatregelen er worden genomen tegen ambtenaren die weigeren een aangifte op te nemen. De leden van de VVD-fractie vragen of de regering bereid is het recht op aangifte nadrukkelijk vast te leggen in dit wetsvoorstel. In reactie daarop stel ik voorop dat het uitgangspunt is dat de politie altijd bereid is tot het opnemen van een melding of aangifte. Uitzondering daarop is dat er evident geen sprake is van een vermoeden van een strafbaar feit. De inzet is dat dit zo laagdrempelig mogelijk is. De politie heeft er baat bij als er zoveel mogelijk aangiften worden gedaan. Wanneer er voldoende aanleiding en bewijs is, kunnen daders worden opgespoord en vervolgd. Ook als niet direct een opsporingsonderzoek gestart kan worden, is een aangifte nog steeds heel belangrijk. Want politie verzamelt en analyseert informatie uit aangiftes altijd. Dit inzicht helpt ons zowel de daders te pakken als het juiste preventiemateriaal te maken.

De politie is op grond van artikel 161 Wetboek van Strafvordering in beginsel verplicht een aangifte op te nemen. Als de politie weigert een aangifte op te nemen kan een klacht worden ingediend, eerst bij de politie en vervolgens bij de officier van justitie.

De beschrijving van het verloop van de informatievoorziening in dit artikel komt de leden van de GroenLinks-fractie nogal gestandaardiseerd over. Volgens deze leden lijken slachtoffers vooral verwezen te worden naar online folders en algemene websites. Daarom vragen deze leden of niet betere en preciezere *tools* voor afzonderlijke groepen slachtoffers ontwikkeld moeten worden om de vaak ingrijpende gevolgen van online financiële criminaliteit en identiteitsmisbruik te (helpen) bestrijden. Zoals hiervoor aangegeven, is het belangrijk dat alle slachtoffers van criminaliteit bij één centraal punt terecht kunnen. Om slachtoffers snel te informeren dat zij bijvoorbeeld contact moeten leggen met hun bank bij bancaire fraude, is het van belang dat deze informatie online wordt aangeboden en als burgers contact opnemen met de politie. Dit gebeurt ook. De politie verwijst slachtoffers daarnaast door naar Slachtofferhulp Nederland (SHN) voor nader praktisch advies, tenzij het slachtoffer aangeeft dat niet te willen. Bovendien beoordeelt de politie bij het opnemen van de aangifte of er sprake is van bijzondere kwetsbaarheid van slachtoffers (individuele beoordeling) en of nog specifieke beschermingsmaatregelen nodig zijn. Wat betreft dat laatste kan gedacht worden aan specifieke voorlichting en tips en doorverwijzing naar meer gespecialiseerde dienstverleners. Vanuit SHN kan hulp op maat worden geboden en worden slachtoffers waar nodig tijdig doorverwezen naar andere instanties zodat zij bijvoorbeeld geen mogelijkheid tot schadeverhaal mislopen bij bijvoorbeeld de bank. De medewerkers van SHN hebben ook op dit terrein van fraude specifieke expertise en bieden emotionele, juridisch en praktische hulp aan slachtoffers. Daarnaast heeft SHN, zoals gezegd, op zijn website een speciale pagina voor hulp na (online) fraude en oplichting. Op deze pagina staat informatie over onder meer oplichting met online aankopen, geldezels, phishing en whatsapp-fraude. Er wordt uitgelegd wat deze vormen van fraude en oplichting inhouden, hoe zij herkend en voorkomen kunnen worden en welke acties het slachtoffer kan ondernemen. SHN biedt voorts slachtoffers de mogelijkheid lotgenoten (online) te ontmoeten. Ook worden slachtoffers verwezen naar instanties en websites die naast SHN specifieke ondersteuning kunnen bieden. Met deze hulp en informatie wordt naar het inzicht van de regering ruim voorzien in bijstand en ondersteuning van deze specifieke groep slachtoffers.

5. Herstel omissie omzetting Richtlijn 2011/93/EU

In het voorstel wordt tevens een omissie bij de omzetting van Richtlijn 2011/93/EU van het Europees Parlement en de Europese Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad hersteld. De leden van de SP-fractie vragen waarom de regering ervoor heeft gekozen de omissie samen met dit wetsvoorstel te combineren en waarom dit niet eerder is gebeurd. Het antwoord daarop is als volgt. Nadat deze omissie aan het licht is gekomen, is deze hersteld in het eerstvolgende wetsvoorstel dat zich voordeed. Dit betrof het onderhavige wetsvoorstel. Bijkomend voordeel is dat het herstel van de omissie op deze manier op redelijk korte termijn kan worden hersteld, gelet op de implementatietermijn van het onderhavige voorstel.

6. Financiële consequenties

De leden van de SP-fractie hebben enkele vragen gesteld ten aanzien van de financiële consequenties van het voorstel. In de memorie van toelichting is daarover inderdaad opgenomen dat van dit wetsvoorstel geen grote extra financiële consequenties worden verwacht en dat de budgettaire gevolgen naar verwachting tot nihil zijn beperkt. Indien zich toch extra kosten voordoen, worden deze binnen de bestaande begrotingen gedekt. Deze leden merken op dat de Nederlandse Vereniging voor Rechtspraak inschat dat het LIRC met meer werk geconfronteerd zal worden en vragen hoe de regering dit verschil in inzicht kan verklaren. Ook vragen deze leden of de regering kan toezeggen dat een eventuele toename van de werkdruk van het LIRC, het Openbaar Ministerie, de politie of rechtspraak ten gevolge van deze wetswijziging kan worden opgevangen zonder dat het ten koste gaat van de bestaande taken. In reactie op de vragen benadruk ik, zoals ook aangegeven in de memorie van toelichting, dat de richtlijn slechts leidt tot aanscherping van een zeer beperkt aantal reeds strafbare gestelde gedragingen. De meeste gedragingen met niet-contante betaalmiddelen die de richtlijn strafbaar stelt, waren reeds strafbaar. De verwachting is niet dat door implementatie van de richtlijn het volume van de internationale informatie-uitwisseling wezenlijk zal toenemen.

De leden van de SGP-fractie stellen terecht dat de politie adequaat en effectief moet kunnen optreden ter bestrijding van de in het voorstel genoemde vormen van fraude. Deze leden vragen wat dit in de praktijk voor de politie en de opleiding aan de Politieacademie betekent.

Het antwoord op deze vraag is dat de meeste gedragingen met niet-contante betaalmiddelen die de richtlijn strafbaar stelt, reeds strafbaar waren in Nederland. In de wet wordt een beperkt aantal wijzigingen voorgesteld. De politie zal via de geëigende wegen de wijzigingen onder de aandacht van haar medewerkers brengen.

II ARTIKELSGEWIJS

Artikel I, onderdelen C en H

Zoals al aangegeven in de inleiding van deze nota hebben de leden van de VVD-fractie met instemming kennisgenomen van de hogere strafmaat voor de in het voorstel genoemde misdrijven. Desalniettemin vragen deze leden de regering waarom is gekozen voor de minimumstraf uit de richtlijn. De leden vragen zich af of dit voorstel niet een goede gelegenheid was geweest de strafmaat aanzienlijk sterker te verhogen en hoe deze keuze is gemaakt in andere lidstaten. Het verheugt mij dat de leden van de VVD-fractie met instemming kennis hebben genomen van de verhoging van de strafmaxima. Voor het antwoord op hun vraag waarom ervoor is gekozen om aan te sluiten bij de minimum-maximumstraffen uit de richtlijn, verwijs ik deze leden graag naar mijn antwoord in paragraaf 4 van deze nota naar aanleiding van het verslag op een soortgelijke vraag van de leden van de SGP-fractie.

Met betrekking tot de gestelde strafmaat in andere lidstaten kan ik melden dat ik hierover op dit moment geen informatie heb. De implementatietermijn van de richtlijn is nog niet verstreken, dus ook andere lidstaten zijn nog bezig met de implementatie van de richtlijn. Ik merk hierbij overigens op dat terughoudend moet worden omgegaan met het maken van een vergelijking tussen de lidstaten, enkel op basis van de verschillende strafhoogten. Zoals in paragraaf 4, in antwoord op een vraag van de leden van de SGP-fractie, aan de orde kwam kennen de strafstelsels (en

strafmaten) in de verschillende lidstaten hun eigen innerlijke coherentie en consistentie. Daarbij is van belang dat de wettelijke strafmaxima niet zonder meer ook de zwaarte of strengheid van de straf reflecteren. Daarop hebben bijvoorbeeld ook de tenuitvoerleggingspraktijk en (in het geval van vrijheidsstraffen) detentieregimes en bijvoorbeeld mogelijkheden voor verlof en vervroegde en voorwaardelijke invrijheidstelling invloed. Daarnaast spelen ook andere factoren een belangrijke rol bij de aanpak van deze vormen van fraude, zoals de pakkans en de inzet op preventie en verstoring van dergelijke activiteiten. In paragraaf 4 van deze nota naar aanleiding van het verslag beschreef ik in antwoord op een vraag van de SGP-fractie al dat deze richtlijn bijdraagt bij aan het vergroten van die pakkans, niet alleen doordat de in de richtlijn opgenomen gedragingen in alle lidstaten strafbaar worden gesteld – hetgeen bijdraagt aan (betere) onderlinge samenwerking bij de opsporing en vervolging –, maar ook door de specifieke voorschriften die in de richtlijn zijn opgenomen over rechtsmacht, de uitwisseling van informatie (met financiële instellingen en met andere lidstaten) en de beschikbaarheid van meldkanalen voor slachtoffers van deze vorm van fraude. De richtlijn draagt eveneens bij aan een betere preventie, onder andere door de bepaling over voorlichtings- en bewustmakingscampagnes.

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