EUROPESE
COMMISSIE

Brussel, 12.9.2018
COM(2018) 637 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

Vrije en eerlijke Europese verkiezingen garanderen

Bijdrage van de Europese Commissie aan de bijeenkomst van de leiders in Salzburg op 20 september 2018

Vrije en eerlijke Europese verkiezingen garanderen

Een cruciaal moment voor de toekomst van de Europese Unie

De essentie van de Europese Unie is het verdedigen van de democratie en de democratische waarden. Dit is noodzakelijk voor een door pluralisme en verdraagzaamheid gevormde samenleving waar de Europese burgers hun stem kunnen uitbrengen in de wetenschap dat zij niet worden misleid. Samen met de rechtsstaat en de grondrechten maakt de democratie ons tot wie wij zijn en definieert zij onze Unie.

De verkiezingen voor het Europees Parlement van mei 2019 zullen plaatsvinden in een geheel andere context dan alle eerdere verkiezingen. De politieke uitdagingen voor de Unie en haar lidstaten zijn enorm. Het is duidelijk dat een robuustere Unie tot stand moet worden gebracht, die geloofwaardigheid en kracht kan bieden op mondiaal niveau, waar rivaliserende machten actief zijn die niet noodzakelijk al onze belangen of waarden delen. Voor een robuuste Unie die berust op doeltreffende justitiële samenwerking, uitwisseling van informatie ter bestrijding van terrorisme en georganiseerde misdaad, en een soepel functionerende interne markt, is vereist dat de lidstaten wederzijds vertrouwen hebben in elkaar en in onze democratische systemen. Tegen deze bijzondere achtergrond vinden de Europese verkiezingen van mei 2019 plaats, die de komende jaren vorm zullen geven aan de toekomst van de Europese Unie.

De weerbaarheid van de democratische stelsels van de Unie moeten worden gewaarborgd. Dat is een onderdeel is van de Veiligheidsunie: aanvallen tegen electorale infrastructuur en campagne-informatiesystemen zijn hybride bedreigingen waartegen de Unie moet optreden. Politiek gemotiveerde massale onlinedesinformatiecampagnes, die ook door derde landen worden georganiseerd, en die specifiek bedoeld zijn om de verkiezingen te discrediteren en de legitimiteit ervan te ondermijnen, blijken onze democratieën in toenemende mate te bedreigen[1]. De Europese Unie moet alles doen wat binnen de grenzen van haar bevoegdheden mogelijk is om haar democratische processen tegen manipulatie door derde landen of particuliere belangen te verdedigen. Verkiezingsperioden blijken bijzonder vatbaar te zijn voor gerichte desinformatie. Dergelijke aanvallen tasten de integriteit en de eerlijkheid van het verkiezingsproces en het vertrouwen van de burgers in verkozen vertegenwoordigers aan en vormen als zodanig een probleem voor de democratie zelf.

De Europese burgers moeten bij het uitbrengen van hun stem een volledig inzicht kunnen krijgen in de politieke keuzes waarvoor zij staan. Dat betekent dat we meer alert moeten zijn op bedreigingen en voor meer transparantie in ons politieke proces moeten zorgen. Een open publieke ruimte, die beveiligd is tegen onrechtmatige beïnvloeding, zorgt voor een gelijk speelveld voor alle politieke campagnes en verkiezingsprocessen, zodat het publiek er vertrouwen in kan stellen[2]. Het is van essentieel belang dat onze democratieën ruimte scheppen voor een levendige politieke campagne, die de kiezers een duidelijk en onvertekend beeld geeft van de ideeën en programma's van de partijen die om hun stem wedijveren. Daarom is het nodig fraude en andere bewuste pogingen om de verkiezingen te manipuleren, actief te bestrijden, onder meer door sancties op te leggen.

[1] Zie de gezamenlijke mededeling aan het Europees Parlement, de Europese Raad en de Raad over het opbouwen van weerbaarheid en reactiecapaciteit tegen hybride bedreigingen (JOIN(2018) 16 final) en de conclusies van de Europese Raad van 28 juni 2018 (https://data.consilium.europa.eu/doc/document/ST-9-2018-INIT/nl/pdf).

[2] De Commissie van Venetië van de Raad van Europa heeft richtsnoeren voor verkiezingen opgesteld (https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev-e), ook wat de media betreft: (https://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2016)006-e).

Onlineactiviteiten zijn aan snelle veranderingen onderhevig, ook tijdens verkiezingen, wat betekent dat betere beveiliging en een gelijk politiek speelveld essentieel zijn. De conventionele („offline") electorale beschermingsmaatregelen, zoals regels voor politieke communicatie tijdens verkiezingsperioden, transparantie van verkiezingsuitgaven en limieten daarvoor, naleving van sperperioden en gelijke behandeling van kandidaten, moeten ook online worden toegepast[3]. Transparantie met betrekking tot politieke reclame op televisie of reclameborden, en limieten die daarvoor gelden, zijn in de onlinewereld net zo goed vereist. Momenteel is dat niet het geval, wat wil zeggen dat dit gemis vóór de volgende Europese verkiezingen moet worden verholpen.

Nieuwe uitdagingen en recente ontwikkelingen

Dankzij onlinecommunicatie ondervinden politieke actoren minder hindernissen en hoeven zij minder kosten te maken voor de interactie met burgers. Zij hebben daardoor meer kansen, maar tegelijkertijd hebben ook kwaadwillige actoren meer mogelijkheden om het democratische debat en de verkiezingsprocessen te beïnvloeden. De onlineomgeving kan het voor actoren gemakkelijker maken om informatie te verstrekken en tegelijkertijd de oorsprong of het doel ervan te verhullen, onder meer door niet transparant te zijn over het feit dat een mededeling (zoals een post op social media) een betaalde advertentie is in plaats van feitelijke rapportage, door opinies als journalistiek te presenteren, of door selectief informatie te presenteren om de gemoederen te verhitten of het debat te polariseren. Niemand moet de illusie koesteren dat de Europese Unie en haar politieke systemen immuun zouden zijn voor dergelijke bedreigingen.

Ook kan de integriteit van de verkiezingen ernstig worden aangetast door „conventionele" cyberincidenten, waaronder cyberaanvallen op verkiezingsprocessen en -campagnes, infrastructuur van politieke partijen, systemen van kandidaten of overheidsinstanties en misbruik van persoonsgegevens. Recente onthullingen, zoals in de zaak Facebook/Cambridge Analytica, zijn een voorbeeld daarvan. In die zaak zijn waarschijnlijk persoonsgegevens misbruikt en onrechtmatig aan derden verstrekt voor heel andere doeleinden dan waarvoor zij oorspronkelijk waren verzameld. Hierdoor is de aandacht gevestigd op de potentiële risico's van bepaalde onlineactiviteiten waarbij burgers illegaal worden benaderd met politieke reclame en communicatie, hun persoonsgegevens onrechtmatig worden verwerkt en misbruikt om hun opinie te manipuleren, desinformatie wordt verspreid of simpelweg de waarheid wordt ondergraven als dat politiek zo uitkomt of verdeeldheid bevordert[4].

---

[3] Zie de recente publicatie *Internet and electoral campaigns – Study on the use of internet in electoral campaigns*, opgesteld door het Committee of experts on Media Pluralism and Transparency of Media Ownership (MSI-MED) van de Raad van Europa (https://rm.coe.int/use-of-internet-in-electoral-campaigns-/16807c0e24). Met de studie is onderzocht wat de gevolgen zijn van de verschuiving van de verkiezingsreclame naar het internet, met name wat betreft electorale uitgaven en reclametechnieken waarbij kiezers gericht worden benaderd met gepersonaliseerde boodschappen. Zie ook Aanbeveling CM/Rec(2016)5 van de Raad van Europa inzake internetvrijheid, waarin wordt verwezen naar de verantwoordelijkheden van overheden, platforms en intermediairs met betrekking tot politieke campagnes van politieke partijen, kandidaten en andere personen online.

[4] Zie het tussentijdse verslag dat de Britse gegevensbeschermingsautoriteit ICO (Information Commissioner's Office) heeft uitgebracht na de opening van een formeel onderzoek naar het gebruik van data-analyse voor politieke doeleinden, dat uitgevoerd werd naar aanleiding van beschuldigingen inzake onrechtmatige gegevensverwerking en gerichte politieke reclame tijdens het referendum over de EU (https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf). In het verslag wordt erop gewezen dat *er door snelle sociale en technologische ontwikkelingen ten aanzien van het gebruik van big data maar weinig bekend (of transparant) is over de „achter de schermen" plaatsvindende gegevensverwerkingstechnieken (zoals algoritmen, analyse, datamatching en profilering) die organisaties en bedrijven gebruiken om personen gericht te benaderen. Wel is duidelijk dat deze methoden*

Ondersteuning van vrije en eerlijke verkiezingen in Europa

De Europese instellingen organiseren geen verkiezingen. De maatregelen in die context vallen primair onder de verantwoordelijkheid van de lidstaten. De lidstaten zijn verantwoordelijk voor de organisatie van de verkiezingen en het toezicht op het verloop van het verkiezingsproces[5]. Er is niettemin een duidelijke EU-dimensie. Door bij de verkiezingen voor het Europees Parlement kandidaten voor te dragen, zijn de nationale en regionale politieke partijen primaire spelers in de Europese verkiezingscampagnes. De Europese politieke partijen en de ermee gelieerde stichtingen spelen een belangrijke rol door op Europees niveau aanvullende campagnes te organiseren, onder meer voor de kandidaten voor de functie van voorzitter van de Europese Commissie.

Na de verkiezingen voor het Europees Parlement van 2014 beloofde de Commissie in haar postelectorale verslag van 2015[6] methoden te onderzoeken om de Europese dimensie en de democratische legitimiteit van het besluitvormingsproces in de Unie verder te versterken en de redenen van de aanhoudend lage opkomst in een aantal lidstaten nader te bestuderen en naar een remedie te zoeken. In februari 2018 heeft de Commissie erop aangedrongen dat vanaf een eerder stadium met de burgers een permanent debat wordt aangegaan over Europese aangelegenheden, dat de politieke partijen vroeger beginnen met hun campagnes voor de Europese verkiezingen, ook wat betreft hun kandidaten voor de functie van voorzitter van de Europese Commissie, dat transparanter wordt omgegaan met de banden tussen nationale en Europese politieke partijen en dat de lidstaten meer bekendheid geven aan het kiesrecht, met name voor ondervertegenwoordigde groepen.

De Europese Unie heeft daarnaast een aantal belangrijke maatregelen getroffen om de democratische weerbaarheid in Europa te versterken, onder meer door middel van het nieuwe Europese kader voor gegevensbescherming dat sinds mei dit jaar van toepassing is. De algemene verordening gegevensbescherming, die inmiddels rechtstreeks van toepassing is in de hele Europese Unie, biedt de noodzakelijke instrumenten om onrechtmatig gebruik van persoonsgegevens aan te pakken, ook in de electorale context. Er wordt ook gewerkt aan de bevordering van een veiliger onlineomgeving door de algehele weerbaarheid tegen cyberaanvallen, waaronder onlinedesinformatie en gedragsmanipulatie, te versterken.

Het is van belang dat zo duidelijk mogelijk wordt gemaakt op welke wijze de Europese gegevensbeschermingsregels in deze nieuwe context moeten worden toegepast, en dat we tegelijkertijd onze inspanningen opvoeren om bewustwording, transparantie en veiligheid te bevorderen. Burgers moeten kunnen vaststellen wat de herkomst is van online tot hen gerichte reclame en politieke boodschappen en door wie een politieke advertentie of een politieke boodschap wordt betaald. Richtsnoeren voor de uitvoering van de nieuwe gegevensbeschermingsregels in de context van de Europese verkiezingen moeten leiden tot meer duidelijkheid en een beter begrip, en bijdragen tot betere samenwerking en informatie-uitwisseling tussen de bevoegde autoriteiten onderling en met andere betrokkenen, en aldus de veiligheid bevorderen.

---

significante gevolgen hebben voor de privacy van de betrokkenen. Het is dus van belang dat er meer echte transparantie komt over het gebruik van deze technieken, zodat mensen de controle over hun gegevens behouden en de wet wordt nageleefd. Als het doel van het gebruik van deze technieken samenhangt met het democratische proces, zijn strenge normen inzake transparantie van zeer groot belang. Ook wordt in het verslag gewezen op het belang dat overwegingen op het gebied van gegevensbescherming beter worden geïntegreerd in het brede regelgevingskader dat voor verkiezingen geldt.

[5] Binnen het kader van de EU-wetgeving en hun internationale verplichtingen.

[6] Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's: Verslag over de verkiezingen voor het Europees Parlement van 2014 (COM(2015) 206 final).

Het maatregelenpakket om de democratische weerbaarheid te versterken, dat samen met deze mededeling wordt gepresenteerd, biedt afgewogen, alomvattende en gerichte acties ter ondersteuning van de integriteit en het doeltreffende verloop van de verkiezingen voor het Europees Parlement van 2019. Alle bij het verkiezingsproces betrokken actoren zijn daarvoor gezamenlijk verantwoordelijk. Dit vereist waakzaamheid en flexibele aanpassing aan een dynamische omgeving en nieuwe technologische ontwikkelingen. De verstrekte richtsnoeren, aanbevelingen en de nodige tools bieden de Europese en nationale politieke partijen, nationale overheden, autoriteiten, particuliere entiteiten en belanghebbenden meer duidelijkheid om gezamenlijk een veiligere democratische omgeving en een gelijk speelveld tot stand te brengen.

De lidstaten worden ook aangemoedigd om de betrokken beginselen toe te passen op andere verkiezingen en referenda die zij op nationaal niveau organiseren.

De voorgestelde maatregelen in het pakket zijn gericht op:

1. het verstrekken van specifieke richtsnoeren inzake de verwerking van persoonsgegevens in het kader van verkiezingen;
2. het aanbevelen van beste praktijken voor het omgaan met risico's die voortvloeien uit desinformatie en cyberaanvallen, het stimuleren van online transparantie en verantwoordingsplicht in het electorale proces in de EU en het versterken van de samenwerking tussen de bevoegde autoriteiten en het voorzien in de middelen om deze in staat te stellen op te treden en zo nodig sancties op te leggen om de integriteit van het verkiezingsproces te waarborgen;
3. het aanpakken van situaties waarin politieke partijen (of de ermee verbonden stichtingen) profiteren van praktijken die in strijd zijn met de gegevensbeschermingsregels om de uitslag van Europese verkiezingen doelbewust te beïnvloeden of te trachten te beïnvloeden.

Bij het voorstellen van dit pakket heeft de Commissie ernaar gestreefd te vermijden dat onnodige administratieve lasten worden opgelegd en dat de handelingsvrijheid van de Europese, nationale en regionale politieke partijen en politieke stichtingen op ongepaste wijze wordt beperkt.

1. Huidige middelen om vrije en eerlijke verkiezingen in de EU te beschermen

De Unie heeft al belangrijke maatregelen getroffen om de integriteit van de verkiezingen te beschermen en het democratische proces te versterken.

Nu de algemene verordening gegevensbescherming (AVG)[7] sinds 25 mei 2018 overal in de Unie rechtstreeks toepasselijk is, is de Europese Unie volledig toegerust om onrechtmatig gebruik van persoonsgegevens te voorkomen en te bestrijden. De Europese Unie zet daarmee op dit gebied de toon.

Bovendien is onlangs ook de Akte betreffende de verkiezing van de leden van het Europees Parlement door middel van rechtstreekse algemene verkiezingen gewijzigd, onder andere om het Europese verkiezingsproces transparanter te maken[8]. De op 3 mei 2018 herziene

[7] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

[8] Besluit (EU, Euratom) 2018/994 van de Raad van 13 juli 2018 tot wijziging van de Akte betreffende de verkiezing van de leden van het Europees Parlement door middel van rechtstreekse algemene verkiezingen,

verordening betreffende het statuut en de financiering van Europese politieke partijen en Europese politieke stichtingen[9] vergroot de erkenning, effectiviteit, transparantie en verantwoordingsplicht van Europese politieke partijen en Europese politieke stichtingen. In Aanbeveling (EU) 2018/234 van de Commissie[10] wordt gewezen op belangrijke stappen om het efficiënte verloop van de verkiezingen voor het Europees Parlement in 2019 te bevorderen.

Richtlijn 2002/58/EG van het Europees Parlement en de Raad (richtlijn betreffende privacy en elektronische communicatie[11]) is van toepassing op ongewenste communicatie voor directmarketingdoeleinden, met inbegrip van politieke berichten die afkomstig zijn van politieke partijen en andere bij het politieke proces betrokken actoren. De richtlijn waarborgt tevens de vertrouwelijkheid en beschermt de informatie die is opgeslagen op de eindapparatuur van de gebruiker, zoals een smartphone of een computer[12]. De voorgestelde richtlijn betreffende privacy en elektronische communicatie[13], waarover momenteel wordt onderhandeld, zorgt voor verdere versterking van de controle die de burger kan uitoefenen, door de transparantie te vergroten en de geboden bescherming uit te breiden tot andere actoren dan de traditionele telecomoperatoren, namelijk elektronischecommunicatiediensten via internet.

Daarnaast heeft de Commissie onlangs een Europese benadering voor de bestrijding van onlinedesinformatie voorgesteld in haar mededeling van 26 april 2018[14]. Met die mededeling wil de Commissie zorgen voor een transparantere, betrouwbaardere en meer verantwoordingsplichtige onlineomgeving. Een belangrijke resultaat dat hiervan wordt verwacht, is de ontwikkeling van een ambitieuze **praktijkcode betreffende desinformatie**, die met name bedoeld is om onlineplatforms en de reclamesector tot transparantie te dwingen en de mogelijkheden voor gerichte politieke reclame te beperken[15]. De code zou in september 2018 moeten worden gepubliceerd[16] en in oktober meetbare resultaten moeten opleveren.

---

gehecht aan Besluit 76/787/EGKS, EEG, Euratom van de Raad van 20 september 1976 (https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32018D0994).

[9] Verordening (EU, Euratom) nr. 1141/2014 van het Europees Parlement en de Raad van 22 oktober 2014 betreffende het statuut en de financiering van Europese politieke partijen en Europese politieke stichtingen (PB L 317 van 4.11.2014, blz. 1).

[10] Aanbeveling (EU) 2018/234 van de Commissie van 14 februari 2018 over het bevorderen van het Europese karakter en het efficiënte verloop van de verkiezingen voor het Europees Parlement in 2019 (PB L 45 van 17.2.2018, blz. 40).

[11] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

[12] De toestemming van de gebruiker is vereist voordat een website toegang krijgt tot dergelijke informatie of het onlinegedrag van de gebruiker mag volgen, bijvoorbeeld door een cookie te plaatsen op de apparatuur van de gebruiker.

[13] Voorstel voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie) (COM(2017) 10 final).

[14] Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's: Bestrijding van onlinedesinformatie: een Europese benadering (COM(2018) 236 final).

[15] Ter voorbereiding op deze praktijkcode heeft de Commissie in mei 2018 een forum georganiseerd dat bestaat uit een werkgroep (waarin de grootste onlineplatforms, de reclamesector en grote adverteerders vertegenwoordigd zijn) en een klankbordgroep (met vertegenwoordigers van de media en maatschappelijke organisaties).

[16] Nadat de klankbordgroep advies heeft uitgebracht.

Meer specifiek is het de bedoeling dat de ondertekenaars van de praktijkcode afspreken om bedrieglijke websites en websites die desinformatie hosten, reclame-inkomsten te ontzeggen, dat zij zorgen voor transparantie ten aanzien van gesponsorde inhoud, met name politieke en thematisch georiënteerde reclame, dat zij duidelijke markeringssystemen en regels opstellen voor het gebruik van bots[17], om te voorkomen dat de activiteiten van bots worden verward met menselijke interactie, en dat zij meer hun best doen om nepaccounts af te sluiten. Daarnaast zouden de ondertekenaars moeten afspreken de ontwikkeling van betrouwbaarheidsindicatoren voor bronnen van inhoud aan te moedigen, zodat inhoud door de gebruikers gemakkelijker kan worden beoordeeld, ervoor te zorgen dat betrouwbare informatie gemakkelijker te vinden is, zodat desinformatie minder zichtbaar wordt, en gebruikers informatie te verstrekken over de wijze waarop door middel van algoritmen de prioriteit van inhoud wordt bepaald. Ook zouden de ondertekenaars betrouwbare organisaties en academische instellingen die feiten controleren toegang moeten bieden tot de platformgegevens. De praktijkcode zal worden beoordeeld in het kader van de werkzaamheden om een actieplan op te stellen met specifieke voorstellen voor een gecoördineerde respons van de EU op desinformatie, dat de Commissie en de hoge vertegenwoordiger voor het einde van het jaar zullen presenteren.

Wat betreft meer „traditionele" cyberincidenten, zoals het hacken van IT-systemen of het bekladden van websites, zijn de definities van de desbetreffende strafbare feiten en de hoogte van de maximumstraffen voor aanvallen op informatiesystemen in de Europese Unie geharmoniseerd bij Richtlijn 2013/40/EU over aanvallen op informatiesystemen.

De bij Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad[18] opgerichte Samenwerkingsgroep heeft de cyberbeveiliging van verkiezingen tot gemeenschappelijke uitdaging bestempeld. Deze Samenwerkingsgroep, waarin de nationale voor cyberbeveiliging bevoegde autoriteiten, de Commissie en het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) zijn vertegenwoordigd, heeft de al bestaande nationale initiatieven inzake de cyberbeveiliging van netwerk- en informatiesystemen die voor verkiezingen worden gebruikt, in kaart gebracht. De Samenwerkingsgroep heeft de met een ontoereikend niveau van cyberbeveiliging voor de komende verkiezingen voor het Europees Parlement gepaard gaande risico's vastgesteld en een compendium voor de cyberbeveiliging van verkiezingstechnologie opgesteld met onder andere technische en organisatorische maatregelen die op basis van ervaringen en beste praktijken zijn opgezet. Het compendium biedt praktische richtsnoeren voor de autoriteiten op het gebied van cyberbeveiliging en de kiescommissies.

2. Zorgen voor meer democratische weerbaarheid: versterking van electorale samenwerkingsnetwerken, onlinetransparantie, bescherming tegen cyberincidenten en bestrijding van desinformatiecampagnes in het kader van de verkiezingen voor het Europees Parlement

Gezien de omvang van de uitdaging en het feit dat de formele verantwoordelijkheden op dit gebied door verschillende instanties worden gedeeld, kunnen zinvolle resultaten slechts door samenwerking van alle betrokken actoren worden bereikt.

[17] Bots plaatsen onder meer geautomatiseerde posts op sociale media en omvatten ook meer interactieve toepassingen, zoals chatbots, die rechtstreeks met de gebruikers in contact staan.

[18] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

Deze mededeling gaat vergezeld van een aanbeveling betreffende electorale samenwerkingsnetwerken, onlinetransparantie, bescherming tegen cyberincidenten en bestrijding van desinformatiecampagnes in het kader van de verkiezingen voor het Europees Parlement. Teneinde vrije en eerlijke verkiezingen te garanderen, zou die aanbeveling geruime tijd voor de verkiezingen voor het Europees Parlement van 2019 moeten worden uitgevoerd door alle betrokken actoren.

In de aanbeveling worden alle lidstaten aangemoedigd een nationaal electoraal netwerk op te zetten en te ondersteunen. De nationale autoriteiten die bevoegd zijn voor verkiezingsaangelegenheden zouden tijdig en doeltreffend moeten samenwerken met instanties op daarmee samenhangende gebieden, zoals gegevensbeschermingsautoriteiten, mediaregulators en autoriteiten voor cyberbeveiliging. Waar nodig zou ook moeten worden samengewerkt met de rechtshandhavingsautoriteiten. Daardoor zullen zij snel eventuele risico's voor de verkiezingen voor het Europees Parlement kunnen opsporen en bestaande regels snel kunnen handhaven, onder meer door financiële sancties op te leggen, bijvoorbeeld door overheidsbijdragen terug te vorderen. De wetgeving van de EU en de lidstaten moet worden nageleefd en gehandhaafd. De Commissie dringt er in dit verband bij de lidstaten op aan dat zij, overeenkomstig het toepasselijke nationale recht en Unierecht, stimuleren dat de gegevensbeschermingsautoriteiten informatie delen met de autoriteiten die belast zijn met het toezicht op de verkiezingen en het toezicht op de activiteiten en de financiering van politieke partijen, indien uit hun besluiten volgt dat een inbreuk verband houdt met de politieke activiteiten van nationale politieke partijen of politieke stichtingen in het kader van de verkiezingen voor het Europees Parlement, of er andere redelijke gronden zijn om zulks aan te nemen.

Ook wordt aanbevolen dat de lidstaten contactpunten aanwijzen voor de deelname aan een Europees netwerk voor samenwerking bij verkiezingen voor het Europees Parlement. De Commissie zal deze samenwerkingsnetwerken ondersteunen door uiterlijk in januari 2019 een eerste bijeenkomst van de aangewezen contactpunten te organiseren. Met inachtneming van de nationale bevoegdheden en de procedurele vereisten die op de betrokken autoriteiten van toepassing zijn, zal dit forum een spilfunctie vervullen voor een Europees realtime waarschuwingsproces en de nationale autoriteiten in de gelegenheid stellen om informatie en praktijken uit te wisselen.

De politieke partijen, politieke stichtingen en campagneorganisaties moeten in hun politieke communicatie met de burgers transparantie waarborgen en ervoor zorgen dat het Europese verkiezingsproces niet door oneerlijke praktijken wordt verstoord. De Commissie presenteert concrete maatregelen ter versterking van de transparantie, zodat burgers zich ervan kunnen vergewissen wie verantwoordelijk is voor de politieke communicatie die zij ontvangen en wie ervoor betaalt[19]. De lidstaten zouden dergelijke transparantie, alsook de inspanningen van de bevoegde autoriteiten op het gebied van het toezicht op inbreuken en de handhaving van de regels, moeten ondersteunen en faciliteren, indien nodig ook door sancties op te leggen. Voor zover relevant, moeten ook de rechtshandhavingsautoriteiten daarbij worden betrokken, zodat een passende reactie op incidenten en passende sancties gewaarborgd zijn[20].

[19] Deze voorstellen vormen een aanvulling op de praktijkcode die momenteel wordt uitgewerkt door het multistakeholderforum dat de Commissie heeft bijeengeroepen naar aanleiding van haar mededeling van 26 april 2018 over onlinedesinformatie.

[20] Dit zou met name van toepassing moeten zijn in gevallen dat een verkiezingsproces met kwaadwillige bedoelingen wordt aangevallen, met inbegrip van incidenten waarbij sprake is van aanvallen op informatiesystemen. Naargelang de omstandigheden kan een strafrechtelijk onderzoek dat tot strafrechtelijke

Weerbaarheid, afschrikking en defensie zijn essentiële elementen voor de totstandkoming van sterke cyberbeveiliging voor de Europese Unie[21]. De bevoegde autoriteiten, politieke partijen, politieke stichtingen en campagneorganisaties op zowel Europees als nationaal niveau moeten zich ten volle bewust zijn van de risico's die de verkiezingen van volgend jaar met zich meebrengen, en passende maatregelen treffen om hun netwerken en informatiesystemen te beschermen[22].

3. Toepassing van de gegevensbeschermingsregels in het kader van het verkiezingsproces

Verordening (EU) 2016/679 van het Europees Parlement en de Raad (algemene verordening gegevensbescherming)[23], die sinds 25 mei 2018 rechtstreeks van toepassing is in de hele Europese Unie, biedt de Unie de noodzakelijke instrumenten om onrechtmatig gebruik van persoonsgegevens in de electorale context aan te pakken.

Aangezien het de allereerste keer is dat deze in de Europese electorale context worden toegepast, namelijk bij de aanstaande verkiezingen voor het Europees Parlement, is het van belang dat het voor alle bij het verkiezingsproces betrokken actoren (zoals de nationale kiesautoriteiten, politieke partijen, gegevensmakelaars, analisten, socialemediaplatforms en onlinereclamenetwerken) duidelijk is hoe de regels het best kunnen worden toegepast en wat op grond ervan al dan niet is toegelaten.

De Commissie heeft daarom specifieke richtsnoeren opgesteld met betrekking tot de verplichtingen op het gebied van gegevensbescherming die in de electorale context relevant zijn. Ter bestrijding van kwaadwillige pogingen om persoonsgegevens te misbruiken, met name met de bedoeling personen gericht te benaderen, moeten de nationale gegevensbeschermingsautoriteiten, die de algemene verordening gegevensbescherming moeten handhaven, ten volle gebruikmaken van hun uitgebreide bevoegdheden om mogelijke inbreuken aan te pakken.

---

sancties leidt, gepast zijn. Zoals eerder vermeld, zijn de definities van strafbare feiten en de hoogte van de maximumstraffen voor aanvallen op informatiesystemen geharmoniseerd bij Richtlijn 2013/40/EU.

[21] In de gezamenlijke mededeling van de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid en de Europese Commissie van september 2017 (JOIN(2017) 450 final) wordt gesteld dat er een alomvattende aanpak moet komen om te bouwen aan sterke cyberbeveiliging voor de Unie op basis van weerbaarheid, afschrikking en defensie.

[22] Het compendium dat is ontwikkeld door de bij Richtlijn (EU) 2016/1148 opgerichte samenwerkingsgroep biedt in dit verband nuttige richtsnoeren. Richtlijn (EU) 2016/1148 heeft als doel een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie tot stand te brengen. Om dat doel te verwezenlijken, voorziet de richtlijn in de ontwikkeling van nationale capaciteiten op het gebied van cyberbeveiliging en de bescherming van essentiële dienstverlening in belangrijke sectoren. Ter versterking van de inspanningen voor een correcte tenuitvoerlegging van de richtlijn verleent de Commissie financiering voor een bedrag van ruim 50 miljoen EUR in de periode tot 2020 via de Connecting Europe Facility. De maatregelen waarin Richtlijn (EU) 2016/1148 voorziet op het gebied van risicobeheersing dienen als relevante benchmarks voor het verkiezingsproces. De algemene verordening gegevensbescherming voorziet ook in de verplichting om passende technische en organisatorische maatregelen te treffen om voor de verwerkte persoonsgegevens een bepaald beveiligingsniveau te waarborgen. Zij is van toepassing op alle bij het verkiezingsproces betrokken actoren en bevat tevens de verplichting om inbreuken in verband met persoonsgegevens te melden aan de bevoegde gegevensbeschermingsautoriteiten en aan de betrokken personen (zie de richtsnoeren van de Commissie).

[23] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

4. Verscherping van de regels inzake de financiering van Europese politieke partijen

Politieke partijen en politieke stichtingen spelen uiteraard een belangrijke rol bij de verkiezingen. Zij wedijveren met hun campagnes om de gunst van de kiezer. Om een gelijk politiek speelveld te garanderen en alle politieke partijen en stichtingen tegen kwaadwillige handelingen te beschermen, moet worden voorkomen dat zich situaties voordoen waarbij een partij kan profiteren van illegale praktijken die een inbreuk op de gegevensbeschermingsregels vormen. Dergelijke praktijken kunnen niet alleen inbreuk maken op de privacy, maar ook in potentie de uitslag van de verkiezingen voor het Europees Parlement beïnvloeden, en moeten daarom worden bestraft. Naast een oproep aan de lidstaten om dergelijke sancties in voorkomend geval ten aanzien van nationale partijen en stichtingen toe te passen, stelt de Commissie een specifieke wijziging van Verordening (EU, Euratom) nr. 1141/2014 voor om te voorzien in evenredige sancties voor gevallen waarbij Europese politieke partijen en stichtingen betrokken zijn. Deze wijziging, die tot verscherping van de bestaande regels strekt, moet waarborgen dat de verkiezingen voor het Europees Parlement kunnen verlopen volgens krachtige democratische regels en met volledige inachtneming van de waarden waarop de Unie berust, in het bijzonder de democratie, de grondrechten en de rechtsstaat.

De Commissie dringt er bij het Europees Parlement en de Raad op aan ervoor te zorgen dat deze gerichte wijzigingen van toepassing zijn voordat de verkiezingen voor het Europees Parlement van 2019 plaatsvinden.

5. Conclusies

Recente gebeurtenissen hebben uitgewezen dat de risico's van manipulatie van het verkiezingsproces door middel van aanvallen op informatiesystemen, misbruik van persoonsgegevens en ondoorzichtige praktijken, reëel en acuut zijn. De EU is daartegen niet immuun. Onlineactiviteiten in de electorale context vormen een nieuwe bedreiging en vergen daarom specifieke beschermingsmaatregelen. De burgers en de democratie worden het best gediend als we er nu voor zorgen dat we voorbereid zijn. Het is te laat als we dergelijke activiteiten na verkiezingen of referenda ontdekken en dan pas maatregelen nemen.

Voor de bescherming van de democratie in de Unie dragen de Europese Unie en haar lidstaten gezamenlijk een plechtige verantwoordelijkheid. Het is bovendien een spoedeisende kwestie. Alle betrokkenen moeten hun inspanningen opvoeren en samenwerken om kwaadwillige inmenging in het electorale systeem af te schrikken, te voorkomen en te bestraffen. De maatregelen die de Commissie in het kader van dit pakket voorstelt, dienen ter ondersteuning van deze inspanningen.

De Commissie zal na de verkiezingen voor het Europees Parlement van 2019 verslag uitbrengen over de uitvoering van de maatregelen in dit pakket.

Volgende stappen voor de verkiezingen voor het Europees Parlement van 2019

- *De Commissie dringt er bij het Europees Parlement en de Raad op aan ervoor te zorgen dat de voorgestelde gerichte wijzigingen van Verordening (EU, Euratom) nr. 1141/2014 tijdig van toepassing zijn, voordat de verkiezingen voor het Europees Parlement van 2019 plaatsvinden.*

- *Samen met de hoge vertegenwoordiger zal de Commissie ondersteuning bieden voor de totstandkoming van een gemeenschappelijke Europese respons op elke buitenlandse inmenging in verkiezingen in de Europese Unie[24]. Naar aanleiding van de conclusies van de Europese Raad van juni 2018 zullen zij in samenwerking met de lidstaten uiterlijk in december 2018 een actieplan presenteren met specifieke voorstellen voor een gecoördineerde respons op het probleem van desinformatie.*

- *De Commissie zal deze kwestie onder de aandacht brengen van de autoriteiten van de lidstaten en met hen in dialoog blijven in het kader van de conferentie op hoog niveau op 15 en 16 oktober 2018 over cyberbedreigingen voor de verkiezingen. De resultaten daarvan zullen als input dienen voor het eerstvolgende colloquium over de grondrechten (26 en 27 november 2018), waarvan het hoofdthema „Democratie in de Europese Unie" is.*

[24] In dat verband zouden tevens de maatregelen kunnen worden toegepast die zijn ontwikkeld krachtens het kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten.