EUROPÄISCHE
KOMMISSION

Brüssel, den 12.9.2018
COM(2018) 637 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

Freie und faire Europawahlen gewährleisten

Ein Beitrag der Europäischen Kommission zum Treffen der Führungsspitzen in Salzburg am 19./20. September 2018

Freie und faire Europawahlen gewährleisten

Ein entscheidender Moment für die Zukunft der Europäischen Union

Demokratie und die Verteidigung der demokratischen Werte sind das Herzstück der Europäischen Union. In einer von Pluralismus und Toleranz geprägten Gesellschaft, in der die Bürgerinnen und Bürger mit der Gewissheit zur Wahlurne schreiten können, nicht irregeführt zu werden, sind diese Werte unerlässlich. Neben der Rechtsstaatlichkeit und den Grundrechten prägt die Demokratie unsere Identität und das Wesen der Union.

Die Wahl zum Europäischen Parlament im Mai 2019 findet in einem ganz anderen Kontext statt als alle bisherigen Wahlen. Die Union und ihre Mitgliedstaaten stehen vor großen politischen Herausforderungen. Auf einer Weltbühne, auf der Akteure um Macht wetteifern, die nicht unbedingt alle unsere Interessen oder Werte teilen, ist es klar geboten, eine robustere Union zu schaffen, die glaubhaft und stark handeln kann. Für eine robuste Union, die auf einer wirksamen justiziellen Zusammenarbeit, dem Austausch von Informationen zur Bekämpfung von Terrorismus und organisierter Kriminalität und einem reibungslos funktionierenden Binnenmarkt aufbaut, sind jeweils gegenseitiges Vertrauen zwischen den Mitgliedstaaten und in unsere demokratischen Systeme erforderlich. Vor diesem außergewöhnlichen Hintergrund wird die Wahl zum Europäischen Parlament im Mai 2019 die Zukunft der Europäischen Union in den kommenden Jahren prägen.

Die Gewährleistung der Widerstandsfähigkeit der demokratischen Systeme der Union ist ein Aufgabenbereich der Sicherheitsunion: Angriffe auf Wahlvorrichtungen und Informationssysteme für Wahlkampagnen sind hybride Bedrohungen, gegen die die Union vorgehen muss. Politisch motivierte Massendesinformationskampagnen im Internet, die auch durch Drittländer gesteuert werden können und eindeutig das Ziel haben, Wahlen die Glaubwürdigkeit und Legitimation zu nehmen, wurden als wachsende Bedrohungen für unsere Demokratien erkannt.[1] Die Europäische Union sollte im Rahmen ihrer Befugnisse alle Maßnahmen ergreifen, um ihre demokratischen Prozesse gegen Manipulationen durch Drittstaaten und private Interessen zu verteidigen. Wahlen haben sich als besonders anfällig für gezielte Desinformation erwiesen. Solche Angriffe beeinträchtigen die Integrität und Fairness des Wahlprozesses und das Vertrauen der Bürger in die gewählten Volksvertreter und stellen damit die Demokratie selbst infrage.

Die europäischen Bürgerinnen und Bürger sollten im vollen Bewusstsein der ihnen offenstehenden politischen Wahlmöglichkeiten wählen können. Dazu sind eine stärkere Sensibilisierung für Bedrohungen und mehr Transparenz in unserem politischen Prozess notwendig. Ein offener öffentlicher Raum, der sicher vor ungebührlicher Beeinflussung schützt, gewährleistet gleiche Ausgangsbedingungen für politische Kampagnen und

[1] Siehe „Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat und den Rat: Stärkung der Resilienz und Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen“ (JOIN(2018) 16 final) und Schlussfolgerungen des Europäischen Rates vom 28. Juni 2018 (http://www.consilium.europa.eu/de/press/press-releases/2018/06/29/20180628-euco-conclusions-final/pdf).

Wahlprozesse, in die die Öffentlichkeit Vertrauen haben kann.[2] Unsere Demokratien müssen Raum für eine dynamische politische Kampagne bieten, die den Wählern ein klares und unverzerrtes Bild der Ideen und Programme der um die Wählergunst werbenden Parteien vermittelt. Daher sollten Betrug und andere bewusste Versuche, die Wahlen zu manipulieren, auch durch Sanktionen aktiv bekämpft werden.

Das Online-Geschehen entwickelt sich auch während Wahlprozessen rasch weiter, sodass eine erhöhte Sicherheit und gleiche Ausgangsbedingungen für die Parteien ganz maßgeblich sind. Daher sollten konventionelle Schutzmaßnahmen, die „offline" Anwendung finden, etwa die Regeln für politische Botschaften während des Wahlkampfs, die Transparenz und Obergrenzen bei den Wahlausgaben, die Einhaltung von Stillhaltefristen und die Gleichbehandlung der Kandidaten auch online gelten.[3] Genauso sollten die bei politischer Werbung im Fernsehen oder auf Wahlplakaten geltenden Transparenzregeln und Beschränkungen für die Online-Welt gelten. Dies ist momentan nicht der Fall, und das muss sich vor den nächsten Wahlen zum Europäischen Parlament ändern.

Neue Herausforderungen und neueste Entwicklungen

Während die Online-Kommunikation auf der einen Seite die Hindernisse und Kosten, mit denen die politischen Akteure konfrontiert sind, wenn sie in den Dialog mit den Bürgern treten wollen, verringert hat und große Chancen bietet, hat sie auf der anderen Seite auch die Möglichkeiten für böswillige Akteure, die demokratische Debatte und die Wahlprozesse zu beeinflussen, erhöht. Das Internet kann es den Akteuren erleichtern, die Herkunft oder den Zweck aufgeführter Informationen zu verschleiern, etwa, indem nicht transparent dargelegt wird, dass eine Mitteilung (wie z. B. ein Post in den sozialen Medien) bezahlte Werbung ist und keine sachliche Berichterstattung, indem Meinungen als journalistische Inhalte dargestellt werden, und indem Berichterstattung selektiv dargeboten wird, um Spannungen zu schüren oder eine Debatte zu polarisieren. Diese Gefahren sollten wir nicht verkennen: Die Europäische Union und ihre politischen Systeme sind nicht immun gegen solche Bedrohungen.

Darüber hinaus können „herkömmliche" Cybervorfälle, z. B. Cyberangriffe auf Wahlprozesse, Kampagnen, Infrastrukturen politischer Parteien, Kandidaten, Systeme der öffentlichen Behörden, und der Missbrauch personenbezogener Daten die Integrität von Wahlen ernsthaft beeinträchtigen. Ein gutes Beispiel hierfür sind die jüngsten Enthüllungen,

[2] Die Venedig-Kommission des Europarates stellt Wahlleitlinien bereit (http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev-e), auch für die Medienlandschaft (http://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2016)006-e).

[3] Siehe die jüngste Veröffentlichung des Europarates zum Thema „Internet und Wahlkampagnen – Studie über die Nutzung des Internets in Wahlkampagnen", erstellt vom Sachverständigenausschuss für Medienpluralismus und Transparenz des Medieneigentums (MSI-MED) des Europarates (https://www.coe.int/en/web/human-rights-rule-of-law/-/internet-and-electoral-campaigns-a-new-study-has-been-published). In der Studie wird untersucht, welche Auswirkungen die Verlagerung der Wahlwerbung ins Internet hat, insbesondere im Hinblick auf die Wahlausgaben und Werbetechniken, die die Wähler gezielt mit personalisierten Botschaften ansprechen („Mikrotargeting"). Siehe auch die Empfehlung des Europarates CM/Rec(2016) 5 zur Internetfreiheit, in der auf die Zuständigkeiten von Regierungen, Plattformen und Intermediären für politische Kampagnen von politischen Parteien, Kandidaten und anderen Einzelpersonen im Internet verwiesen wird.

etwa im Fall „Facebook/Cambridge Analytica“. Es ist davon auszugehen, dass personenbezogene Daten missbräuchlich verwendet und für ganz andere als die ursprünglich beabsichtigten Zwecke rechtswidrig an Dritte weitergegeben wurden. Dies hat die Gefahren bestimmter Online-Aktivitäten aufgezeigt, die gezielt dazu eingesetzt werden, Bürgerinnen und Bürger heimlich mit politischer Werbung und politischen Botschaften zu beeinflussen, deren personenbezogene Daten rechtswidrig zu verarbeiten und zu missbrauchen, um Meinungen zu manipulieren, Desinformation zu verbreiten oder einfach nur die Wahrheit zu verschleiern, wenn dies politischen Zwecken dient oder Gräben vertieft.[4]

Freie und faire Wahlen in Europa fördern

Die europäischen Organe führen keine Wahlen durch. Die entsprechende Zuständigkeit liegt nach wie vor in erster Linie bei den Mitgliedstaaten. Es ist demnach Sache der Mitgliedstaaten, Wahlen zu organisieren und die Durchführung des Wahlprozesses zu beobachten.[5] Dennoch gibt es einen klaren Bezug zur Unionsebene. Denn indem nationale und regionale politische Parteien Kandidaten für die Wahlen zum Europäischen Parlament vorschlagen, werden sie zu zentralen Akteuren in den europäischen Wahlkampagnen. Den europäischen politischen Parteien und ihren parteinahen Stiftungen kommt bei der Organisation begleitender Kampagnen auf europäischer Ebene, einschließlich der Kampagnen für die Spitzenkandidaten für das Amt des Präsidenten der Europäischen Kommission, eine wichtige Rolle zu.

Nach der Wahl zum Europäischen Parlament 2014 hatte die Kommission in ihrem Wahlbericht von 2015[6] betont, dass es wichtig ist, „die Möglichkeiten zur nochmaligen Stärkung der europäischen Dimension und der demokratischen Legitimität der politischen Willensbildung der EU auszuloten und die Gründe für die anhaltend geringe Wahlbeteiligung in einigen Mitgliedstaaten weiter zu prüfen und anzugehen.“ Im Februar 2018 rief die Kommission dazu auf, frühzeitig und kontinuierlich mit den Bürgerinnen und Bürgern in den Dialog über europäische Themen zu treten, die Kampagnen der politischen Parteien für die Wahlen zum Europäischen Parlament – einschließlich der Kampagnen für deren Kandidaten für das Amt des Präsidenten der Europäischen Kommission – früher einzuleiten, die

[4] Siehe den von der britischen Datenschutzbehörde (ICO) veröffentlichten Zwischenbericht nach der Einleitung eines förmlichen Prüfverfahrens wegen der Verwendung von Datenanalysen für politische Zwecke, nachdem Vorwürfe hinsichtlich einer widerrechtlichen Verarbeitung von Daten und des Mikrotargeting von politischer Werbung während des EU-Referendums erhoben wurden (https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf). In dem Bericht wird hervorgehoben, dass *„die raschen sozialen und technologischen Entwicklungen bei der Verwendung von Massendaten zur Folge haben, dass die Datenverarbeitungsmethoden im Hintergrund (einschließlich Algorithmen, Analysen, Datenabgleichungen und Profiling), die von Organisationen und Unternehmen zum Mikrotargeting von Einzelpersonen genutzt werden, nur wenig bekannt und wenig transparent sind. Klar ist jedoch, dass diese Instrumente einen großen Einfluss auf die Privatsphäre der Menschen haben können. Es ist wichtig, bei der Verwendung solcher Techniken eine größere und echte Transparenz walten zu lassen, um sicherzustellen, dass die Menschen die Kontrolle über ihre eigenen Daten haben und das Gesetz eingehalten wird. Wenn diese Methoden zum Zwecke der Beeinflussung des demokratischen Prozesses verwendet werden, sind hohe Transparenzstandards unentbehrlich.“* Auch wird darauf hingewiesen, wie wichtig es ist, Datenschutzerwägungen stärker in den allgemeineren Rechtsrahmen für Wahlen zu integrieren.

[5] Im Rahmen des EU-Rechts und der internationalen Verpflichtungen.

[6] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Bericht über die Wahlen zum Europäischen Parlament 2014 (COM(2015) 206 final).

Zusammenhänge zwischen nationalen und europäischen politischen Parteien transparenter darzulegen und das Wahlrecht, insbesondere für unterrepräsentierte Gruppen, auf nationaler Ebene zu fördern.

Die Europäische Union hat auch bereits einige wichtige Schritte zum Aufbau von demokratischer Resilienz in Europa unternommen, etwa mit dem neuen europäischen Datenschutzrahmen, der seit Mai dieses Jahres in Kraft ist. Diese Datenschutz-Grundverordnung, die in der gesamten Europäischen Union unmittelbar gilt, stellt die Instrumente bereit, die für den Umgang mit Fällen von widerrechtlicher Nutzung personenbezogener Daten im Wahlkontext erforderlich sind. Auch wird daran gearbeitet, unsere allgemeine Widerstandsfähigkeit gegen Cyberbedrohungen, u. a. gegen Desinformation im Internet und Verhaltensmanipulation, zu stärken und damit ein sichereres Online-Umfeld zu fördern.

Es muss möglichst klar sein, wie die europäischen Datenschutzvorschriften in diesem neuen Kontext umzusetzen sind; gleichzeitig müssen wir noch mehr dafür tun, das Bewusstsein, die Transparenz und die Sicherheit zu erhöhen. Die Bürgerinnen und Bürger sollten erkennen können, wer sich im Internet mit politischer Werbung oder politischen Botschaften an sie wendet und wer diese Werbeanzeigen und Botschaften finanziert. Die Leitlinien zur Umsetzung der neuen Datenschutzbestimmungen im Rahmen der Europawahlen dürften zu mehr Klarheit und einem besseren Verständnis beitragen, während eine stärkere Zusammenarbeit und ein besserer Informationsaustausch zwischen den zuständigen Behörden und mit anderen Akteuren die Sicherheit erhöhen.

Das zusammen mit dieser Mitteilung vorgelegte Paket zur Stärkung der demokratischen Resilienz enthält ausgewogene, umfassende und gezielte Maßnahmen zur Unterstützung der Integrität und der wirksamen Durchführung der Wahl zum Europäischen Parlament 2019 – eine gemeinsame Aufgabe aller am Wahlprozess beteiligten Akteure, die ständige Wachsamkeit und eine flexible Anpassung an ein dynamisches Umfeld und neue technologische Entwicklungen erfordert. Durch die Bereitstellung von Leitlinien, Empfehlungen und der notwendigen Instrumente herrscht bei den europäischen und nationalen politischen Parteien, den nationalen Regierungen, den Behörden, den privaten Stellen und den Interessenträgern mehr Klarheit, um gemeinsam ein sichereres demokratisches Umfeld und gleiche Ausgangsbedingungen zu schaffen.

Die Mitgliedstaaten sind auch angehalten, diese Grundsätze auf andere Wahlen und Referenden, die sie auf nationaler Ebene organisieren, anzuwenden.

Die in diesem Paket vorgeschlagenen Maßnahmen zielen auf Folgendes ab:

1. Bereitstellung spezifischer Leitlinien für die Verarbeitung personenbezogener Daten bei Wahlen;
2. Empfehlungen von bewährten Verfahren für den Umgang mit den Gefahren von Desinformation und Cyberangriffen und für die Förderung von Transparenz und Rechenschaftspflicht im Internet im EU-Wahlprozess; Schutz der Integrität des

Wahlprozesses durch Ausbau der Zusammenarbeit zwischen den zuständigen Behörden und Einrichtung der erforderlichen Instrumente, um bei Bedarf eingreifen und Sanktionen verhängen zu können;

3. Umgang mit Situationen, in denen politische Parteien oder parteinahe Stiftungen datenschutzrechtswidrige Praktiken nutzen, um das Ergebnis der Wahlen zum Europäischen Parlament bewusst zu beeinflussen oder dies zu versuchen.

Bei der Vorlage dieses Pakets hat die Kommission darauf geachtet, unnötigen Verwaltungsaufwand zu vermeiden und den Handlungsspielraum für europäische, regionale und nationale politische Parteien und Stiftungen nicht unzweckmäßig zu beschränken.

1. Aktuelle EU-Schutzmaßnahmen zur Gewährleistung freier und fairer Wahlen

Die Union hat bereits wichtige Schritte unternommen, um die Integrität der Wahlen zu schützen und den demokratischen Prozess zu konsolidieren.

Mit der seit dem 25. Mai 2018 in der gesamten Union unmittelbar geltenden Datenschutz-Grundverordnung (DSGVO)[7] ist die Europäische Union nun bestens gerüstet, um die widerrechtliche Verwendung personenbezogener Daten zu verhindern bzw. dagegen vorzugehen. Die Europäische Union setzt damit in diesem Bereich neue Standards.

Zudem wurde der Rechtsakt zu den Wahlen der Mitglieder des Europäischen Parlaments kürzlich geändert, um u. a. die Transparenz im europäischen Wahlprozess zu erhöhen.[8] Die am 3. Mai 2018 angenommene überarbeitete Verordnung über das Statut und die Finanzierung europäischer politischer Parteien[9] erhöht die Anerkennung, Wirksamkeit, Transparenz und Rechenschaftspflicht europäischer politischer Parteien und europäischer politischer Stiftungen. In der Empfehlung (EU) 2018/234 der Kommission[10] werden wichtige Schritte für eine noch effizientere Durchführung der Wahlen zum Europäischen Parlament 2019 aufgezeigt.

Die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (Datenschutzrichtlinie für elektronische Kommunikation[11]) findet Anwendung bei unerbetenen Nachrichten zum

[7] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

[8] Beschluss (EU, Euratom) 2018/994 des Rates vom 13. Juli 2018 zur Änderung des dem Beschluss 76/787/EGKS, EWG, Euratom des Rates vom 20. September 1976 beigefügten Akts zur Einführung allgemeiner unmittelbarer Wahlen der Mitglieder des Europäischen Parlaments (https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018D0994&qid=1531826494620)

[9] Verordnung (EU, Euratom) Nr. 1141/2014 des Europäischen Parlaments und des Rates vom 22. Oktober 2014 über das Statut und die Finanzierung europäischer politischer Parteien und europäischer politischer Stiftungen (ABl. L 317 vom 4.11.2014, S. 1).

[10] Empfehlung (EU) 2018/234 der Kommission vom 14. Februar 2018 zur Stärkung des europäischen Charakters und der effizienten Durchführung der Wahlen 2019 zum Europäischen Parlament (ABl. L 45 vom 17.2.2018, S. 40).

[11] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

Zweck der Direktwerbung, darunter politische Botschaften, die von politischen Parteien und anderen am politischen Prozess beteiligten Akteuren übermittelt werden. Sie gewährleistet auch die Vertraulichkeit und den Schutz der auf dem Endgerät eines Nutzers, etwa einem Smartphone oder einem Computer, gespeicherten Daten.[12] Die vorgeschlagene Verordnung über Privatsphäre und elektronische Kommunikation[13], über die derzeit verhandelt wird, wird den Bürgern noch mehr Kontrolle einräumen, indem die Transparenz erhöht und der Schutz über die herkömmlichen Telekommunikationsbetreiber hinaus auf internetgestützte elektronische Kommunikationsdienste ausgeweitet wird.

Darüber hinaus hat die Kommission jüngst in ihrer Mitteilung vom 26. April 2018 ein europäisches Konzept zur Bekämpfung von Desinformation im Internet vorgestellt.[14] Mit dieser Mitteilung möchte die Kommission ein transparenteres, vertrauenswürdigeres und verantwortungsvolleres Online-Umfeld fördern. Eines der wichtigsten Projekte ist die Ausarbeitung eines ehrgeizigen **Verhaltenskodex für den Bereich der Desinformation**, der insbesondere Online-Plattformen und die Werbewirtschaft dazu bringen soll, Transparenz zu gewährleisten und die Möglichkeiten der Nutzung von Zielgruppen-Profilen für politische Werbung zu beschränken.[15] Der Kodex soll im September 2018 veröffentlicht werden[16] und bis Oktober messbare Ergebnisse liefern.

Insbesondere sollten sich die Unterzeichner des Verhaltenskodex darauf einigen, „Hochstapler"-Websites und Websites mit Desinformation die Werbeeinnahmen zu entziehen und im Zusammenhang mit gesponserten Inhalten für Transparenz zu sorgen, insbesondere bei politischer und themenbezogener Werbung; zudem sollten sie klare Kennzeichnungsregeln und -systeme für Bots[17] erstellen, damit deren Tätigkeiten nicht mit menschlicher Interaktion verwechselt werden können, und die Bemühungen zur Schließung von Scheinkonten intensivieren. Die Unterzeichner sollten sich ferner darauf einigen, die Nutzerbewertung von Inhalten zu erleichtern, indem sie die Entwicklung von Indikatoren für die Vertrauenswürdigkeit von Inhaltsquellen fördern, die Sichtbarkeit von Desinformation durch eine bessere Auffindbarkeit vertrauenswürdiger Inhalte verringern und die Nutzer über die Priorisierung von Inhalten durch Algorithmen aufklären. Darüber hinaus sollten die Unterzeichner vertrauenswürdigen Organisationen und Hochschulen, die Fakten prüfen, Zugang zu den Plattformdaten gewähren. Der Verhaltenskodex wird im Rahmen der

[12] Bevor die Websites Zugang zu solchen Informationen erhalten oder das Online-Verhalten eines Nutzers, z. B. durch die Speicherung von Cookies auf dessen Gerät, verfolgen können, muss der Nutzer seine Einwilligung geben.
[13] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017) 10 final).
[14] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Bekämpfung von Desinformation im Internet: ein europäisches Konzept" (COM(2018) 236 final).
[15] Zur Vorbereitung dieses Verhaltenskodex berief die Kommission im Mai 2018 ein Forum ein, das sich aus einer „Arbeitsgruppe" (mit den wichtigsten Online-Plattformen und Vertretern der Werbewirtschaft sowie größeren Werbetreibenden) und einem „Sounding Board" (aus Medienvertretern und Vertretern der Zivilgesellschaft) zusammensetzt.
[16] Nachdem das Sounding Board seine Stellungnahme abgegeben hat.
[17] Zu den Bots gehört das automatische Posten von Nachrichten auf Plattformen der sozialen Medien, aber auch interaktivere Anwendungen wie Chatbots, die direkt mit den Nutzern interagieren.

Ausarbeitung eines Aktionsplans mit spezifischen Vorschlägen für eine koordinierte Reaktion der EU auf die Herausforderung der Desinformation bewertet; die Kommission und die Hohe Vertreterin sollen diese Bewertung vor Jahresende vorlegen.

Was die „traditionelleren" Cybervorfälle betrifft, etwa das Hacken von IT-Systemen oder das Verunstalten von Websites, so wurden mit der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme die Definitionen von Straftatbeständen und Mindeststrafen für Angriffe auf Informationssysteme auf EU-Ebene harmonisiert.

Die im Rahmen der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[18] eingesetzte Kooperationsgruppe hat die Cybersicherheit bei Wahlen als gemeinsame Herausforderung erkannt. Diese Gruppe, zu der die für Cybersicherheit zuständigen nationalen Behörden, die Kommission und die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) gehören, hat die nationalen Initiativen, die es im Bereich Cybersicherheit von für Wahlen genutzten Netz- und Informationssystemen gibt, erfasst. Sie hat ermittelt, welche Risiken von einer mangelhaften Cybersicherheit für die nächsten Wahlen zum Europäischen Parlament ausgehen und ein Kompendium zur Computer- und Netzsicherheit von Wahltechnologie erarbeitet, das auch auf Erfahrungen und bewährten Vorgehensweisen basierende technische und organisatorische Maßnahmen umfasst. Das Kompendium enthält praktische Hinweise für Cybersicherheitsbehörden und Wahlgremien.

2. Ausbau der demokratischen Resilienz: bessere Kooperationsnetze, mehr Online-Transparenz, ein besserer Schutz vor Cybersicherheitsvorfällen und eine stärkere Bekämpfung von Desinformationskampagnen im Zusammenhang mit den Wahlen zum Europäischen Parlament

Angesichts der Tragweite der Herausforderung und der Tatsache, dass sich in diesem Bereich formell mehrere Behörden die Zuständigkeiten teilen, können nur dann bedeutsame Ergebnisse erzielt werden, wenn alle beteiligten Akteure an einem Strang ziehen.

Flankiert wird die Mitteilung von einer Empfehlung zu Wahlkooperationsnetzen, zu Online-Transparenz, zum Schutz vor Cybersicherheitsvorfällen und zur Bekämpfung von Desinformationskampagnen im Zusammenhang mit Wahlen zum Europäischen Parlament. Um freie und faire Wahlen zu gewährleisten, sollte die Empfehlung frühzeitig vor der Wahl zum Europäischen Parlament 2019 von allen Akteuren umgesetzt werden.

In der Empfehlung wird jeder Mitgliedstaat aufgefordert, ein nationales Wahlnetz einzurichten und zu unterstützen. Die für Wahlfragen zuständigen Behörden der Mitgliedstaaten sollten mit Behörden, deren Arbeit damit zusammenhängt (z. B.

[18] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

Datenschutzbehörden, Medienaufsichtsbehörden, Cybersicherheitsbehörden usw.) zeitnah und effektiv zusammenarbeiten. Bei Bedarf sollten sie auch mit Strafverfolgungsbehörden zusammenarbeiten. Auf diese Weise können sie rasch potenzielle Bedrohungen für die Wahlen zum Europäischen Parlament erkennen und bestehende Vorschriften, etwa mögliche finanzielle Sanktionen wie die Rückzahlung des öffentlichen Beitrags, zeitnah durchsetzen. Die Rechtsvorschriften der EU und der Mitgliedstaaten müssen eingehalten und durchgesetzt werden. In diesem Zusammenhang fordert die Kommission die Mitgliedstaaten auf, im Einklang mit dem geltenden nationalen und Unionsrecht die Weitergabe von Informationen durch die Datenschutzbehörden an die für die Wahlbeobachtung und die Überwachung von Tätigkeiten und Finanzierung politischer Parteien zuständigen Behörden zu fördern, wenn sich aus ihren Entscheidungen schlussfolgern lässt oder es hinreichende Gründe für die Annahme gibt, dass ein Verstoß mit politischen Tätigkeiten von nationalen politischen Parteien oder Stiftungen im Rahmen der Wahlen zum Europäischen Parlament zusammenhängt.

Ferner wird empfohlen, dass die Mitgliedstaaten Kontaktstellen benennen, die sich an einem europäischen Kooperationsnetz für die Wahlen zum Europäischen Parlament beteiligen. Die Kommission wird diese Kooperationsnetze unterstützen und eine erste Sitzung der benannten Kontaktstellen bis Januar 2019 einberufen. Dieses Forum wird unter Achtung der nationalen Zuständigkeiten und der für die jeweiligen Behörden geltenden Verfahrensvorschriften das Kernstück eines europäischen Warnmechanismus in Echtzeit bilden und eine Plattform für den Informations- und Erfahrungsaustausch zwischen den Behörden der Mitgliedstaaten bieten.

Politische Parteien, Stiftungen und Wahlkampfeinrichtungen müssen bei ihren politischen Botschaften an die Bürger transparente Verfahren gewährleisten und sicherstellen, dass der europäische Wahlprozess nicht durch unlautere Praktiken verzerrt wird. Die Kommission legt konkrete Maßnahmen zur Stärkung der Transparenz vor, die gewährleisten sollen, dass die Bürger erkennen können, wer hinter den an sie gerichteten politischen Botschaften steht und wer sie finanziert.[19] Die Mitgliedstaaten sollten diese Transparenz und die Bemühungen der zuständigen Behörden, Verstöße zu überwachen, Vorschriften durchzusetzen und bei Bedarf auch Sanktionen zu verhängen, unterstützen und erleichtern. Gegebenenfalls sollten auch Strafverfolgungsbehörden einbezogen werden, um eine angemessene Reaktion auf Vorfälle und entsprechende Sanktionen zu gewährleisten.[20]

[19] Ergänzt werden die Vorschläge durch den Verhaltenskodex, der vom von der Kommission nach ihrer Mitteilung vom 26. April 2018 über Desinformation im Internet einberufenen Stakeholder-Forum ausgearbeitet wird.

[20] Dies würde insbesondere Fälle betreffen, in denen ein Wahlverfahren mutwillig manipuliert wird, wozu auch Angriffe auf Informationssysteme zählen. Je nach den Umständen können strafrechtliche Ermittlungen, die zu strafrechtlichen Sanktionen führen können, angebracht sein. Wie bereits erwähnt, wurden die Definitionen von Straftatbeständen und Mindeststrafen für Angriffe auf Informationssysteme mit der Richtlinie 2013/40/EU harmonisiert.

Die Grundpfeiler für den Aufbau einer starken Cybersicherheit für die Europäische Union sind Abwehrfähigkeit, Abschreckung und Abwehr.[21] Die zuständigen europäischen und nationalen Behörden, politischen Parteien, Stiftungen und Wahlkampforganisationen sollten sich der Risiken für die Wahlen nächstes Jahr in vollem Maße bewusst sein und angemessene Anstrengungen zum Schutz ihrer Netz- und Informationssysteme unternehmen.[22]

3. Anwendung von Datenschutzbestimmungen im Wahlprozess

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung)[23], die seit dem 25. Mai 2018 unmittelbar in der gesamten Union gilt, stellt der Union die Instrumente zur Verfügung, die für den Umgang mit Fällen von widerrechtlicher Nutzung personenbezogener Daten im Wahlkontext erforderlich sind.

Da die Datenschutzbestimmungen zum ersten Mal im Rahmen der Wahlen zum Europäischen Parlament Anwendung finden werden, ist es wichtig, dass alle an den Wahlen beteiligten Akteure – d. h. die nationalen Wahlbehörden, die politischen Parteien, die Datenvermittler und Analysten, die Social-Media-Plattformen und Online-Werbenetzwerke – wissen, wie die Vorschriften am besten angewandt werden sollten und was zulässig ist und was nicht.

Die Kommission hat daher spezifische Leitlinien ausgearbeitet, um die für Wahlen wichtigen Datenschutzverpflichtungen zusammenzustellen. Um böswillige Versuche, personenbezogene Daten insbesondere zum Zwecke des Mikrotargeting zu missbrauchen, müssen die nationalen Datenschutzbehörden, deren Aufgabe die Durchsetzung der Datenschutz-Grundverordnung ist, ihre erweiterten Befugnisse in vollem Maße nutzen, um mögliche Verstöße zu ahnden.

4. Strengere Vorschriften für die Finanzierung europäischer politischer Parteien

[21] In der gemeinsamen Mitteilung der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik und der Europäischen Kommission vom September 2017 wird anerkannt, dass für den Aufbau einer starken Cybersicherheit für die Union ein umfassender Ansatz erforderlich ist, der auf Abwehrfähigkeit, Abschreckung und Abwehr setzt (JOIN(2017) 450 final).

[22] Das Kompendium, das von der mit der Richtlinie (EU) 2016/1148 eingesetzten Kooperationsgruppe entwickelt wurde, liefert diesbezüglich nützliche Hinweise. Die Richtlinie (EU) 2016/1148 zielt darauf ab, unionsweit ein hohes Maß an Resilienz im Bereich der Cybersicherheit zu erreichen. Dazu werden mit der Richtlinie der Aufbau nationaler Cybersicherheitskapazitäten gefördert und die Erbringung wesentlicher Dienste in Schlüsselbereichen geschützt. Um die Bemühungen um eine ordnungsgemäße Umsetzung der Richtlinie zu verstärken, stellt die Kommission über die Fazilität „Connecting Europe“ (CEF) bis 2020 Finanzmittel in Höhe von über 50 Mio. EUR bereit. Die in der Richtlinie (EU) 2016/1148 vorgesehenen Risikomanagementmaßnahmen sind wichtige Benchmarks für den Wahlprozess. Zur Gewährleistung der Sicherheit bei der Verarbeitung personenbezogener Daten sieht die Datenschutz-Grundverordnung ferner die Verpflichtung vor, geeignete technische und organisatorische Maßnahmen durchzuführen. Sie gilt für alle an den Wahlen beteiligten Akteure und schreibt auch vor, Verstöße gegen den Schutz personenbezogener Daten an die zuständigen Datenschutzbehörden und die betroffenen Personen weiterzuleiten (siehe Leitfaden der Kommission).

[23] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

Politische Parteien und Stiftungen stehen bei Wahlen natürlich im Mittelpunkt des Geschehens. Über ihre Wahlkampagnen werben sie um die Gunst der Wähler. Um gleiche Ausgangsbedingungen zu gewährleisten und alle politischen Parteien und Stiftungen vor gegen sie gerichteten Vergehen zu schützen, müssen unbedingt Situationen vermieden werden, in denen eine Partei von widerrechtlichen Praktiken, die gegen die Datenschutzvorschriften verstoßen, profitiert. Es sollten Sanktionen gegen diejenigen verhängt werden, die nicht nur die Privatsphäre von Personen verletzen, sondern dies in einer Weise tun, die auch das Ergebnis der Wahlen zum Europäischen Parlament beeinflussen könnte. Neben einer Aufforderung an die Mitgliedstaaten, gegebenenfalls entsprechende Sanktionen gegen nationale Parteien und Stiftungen zu verhängen, schlägt die Kommission vor, die Verordnung (EU, Euratom) Nr. 1141/2014 gezielt dahin gehend zu ändern, dass auch in Fällen, in denen europäische politische Parteien und Stiftungen betroffen sind, angemessene Sanktionen vorgesehen sind. Mit dieser Änderung, die die bestehenden Vorschriften stärkt, soll sichergestellt werden, dass die Wahlen zum Europäischen Parlament im Einklang mit strengen demokratischen Regeln und unter uneingeschränkter Achtung der Werte, auf die sich die Union gründet, insbesondere Demokratie, Grundrechte und Rechtsstaatlichkeit, abgehalten werden können.

Die Kommission fordert das Europäische Parlament und den Rat eindringlich auf, dafür Sorge zu tragen, dass diese gezielten Änderungen noch vor der Wahl zum Europäischen Parlament im Jahr 2019 eingeführt werden.

5. Schlussfolgerungen

Die jüngsten Ereignisse haben gezeigt, dass die Gefahr einer Manipulation des Wahlprozesses, sei es durch Angriffe auf Informationssysteme, den Missbrauch personenbezogener Daten oder undurchsichtige Praktiken, real und akut ist. Die EU ist dagegen nicht immun. Online-Aktivitäten im Kontext von Wahlen stellen eine neuartige Bedrohung dar und erfordern einen gezielten Schutz. Am besten dienen wir den Bürgerinnen und Bürgern und der Demokratie, wenn wir jetzt Vorbereitungen treffen. Wir können damit nicht bis nach den Wahlen oder Referenden warten, um nachträglich solche Aktivitäten festzustellen und erst dann darauf zu reagieren.

Der Schutz der Demokratie in der Union ist eine gemeinsame und ehrenvolle Aufgabe der Europäischen Union und ihrer Mitgliedstaaten. Und die Zeit drängt. Alle beteiligten Akteure müssen ihre Anstrengungen verstärken und zusammenarbeiten, um böswillige Eingriffe in das Wahlsystem zu unterbinden, abzuwehren und zu sanktionieren. Die von der Kommission in diesem Paket vorgeschlagenen Maßnahmen unterstützen diese Bemühungen.

Nach der Wahl zum Europäischen Parlament 2019 wird die Kommission einen Bericht über die Umsetzung dieses Maßnahmenpakets vorlegen.

<u>Nächste Schritte im Vorfeld der Wahl zum Europäischen Parlament 2019</u>

- *Die Kommission fordert das Europäische Parlament und den Rat eindringlich auf, dafür Sorge zu tragen, dass die vorgeschlagenen gezielten Änderungen an der Verordnung (EU, Euratom) Nr. 1141/2014 rechtzeitig für die Wahl zum Europäischen Parlament im Jahr 2019 in Kraft sind.*

- *Zusammen mit der Hohen Vertreterin wird die Kommission die Ausarbeitung gemeinsamer europäischer Reaktionen auf eine etwaige ausländische Einmischung in Wahlen in der Europäischen Union unterstützen.*[24] *Entsprechend den Schlussfolgerungen des Europäischen Rates vom Juni 2018 werden die beiden Organe in Zusammenarbeit mit den Mitgliedstaaten bis Dezember 2018 einen Aktionsplan vorlegen, der konkrete Vorschläge für eine koordinierte Reaktion der EU auf die Herausforderung der Desinformation enthält.*

- *Mit der hochrangigen Konferenz über Cyberbedrohungen für Wahlen, die am 15. und 16. Oktober 2018 stattfindet, wird die Kommission für das Thema sensibilisieren und ihren Dialog mit den Behörden der Mitgliedstaaten fortsetzen; die Ergebnisse der Konferenz werden in das nächste Kolloquium über Grundrechte (26./27. November 2018) mit dem Schwerpunkt „Demokratie in der Europäischen Union" einfließen.*

[24] Dies kann auch Maßnahmen umfassen, die für den Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten ausgearbeitet wurden.