KOMISJA
EUROPEJSKA

Bruksela, dnia 12.9.2018 r.
COM(2018) 637 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

Zapewnienie wolnych i uczciwych wyborów europejskich

Wkład Komisji Europejskiej na spotkanie przywódców w Salzburgu w dniach 19-20 września 2018 r.

Zapewnienie wolnych i uczciwych wyborów europejskich

Kluczowy moment dla przyszłości Unii Europejskiej

Unia Europejska jest po to, by stać na straży demokracji i wartości demokratycznych. Demokracja i związane z nią wartości są w pluralistycznym i tolerancyjnym społeczeństwie niezbędne. Służą one temu, by obywatele Unii mogli brać udział w wyborach z pełnym przekonaniem, że nie są manipulowani. Demokracja, praworządność i prawa podstawowe są częścią naszej tożsamości i definiują Unię.

Wybory do Parlamentu Europejskiego, które odbędą się w maju 2019 r., będą przebiegały w diametralnie innym kontekście niż wszystkie poprzednie wybory. Unia i jej państwa członkowskie stoją przed ogromnymi wyzwaniami. Niewątpliwie istnieje potrzeba wzmocnienia Unii, tak aby stała się wiarygodnym i silnym graczem na arenie międzynarodowej, zdolnym do konkurowania z potęgami światowymi, które dążąc do zwiększenia swojego znaczenia, niekoniecznie kierują się zbieżnymi z naszymi interesami lub wartościami. Silna Unia oparta na skutecznej współpracy sądowej, wymianie informacji służących zwalczaniu terroryzmu i przestępczości zorganizowanej oraz na sprawnie funkcjonującym rynku wewnętrznym – to wszystko wymaga wzajemnego zaufania między państwami członkowskimi oraz w ramach ich systemów demokratycznych. W tym wyjątkowym kontekście wybory do Parlamentu Europejskiego, które odbędą się w maju 2019 r., określą przyszłość Unii Europejskiej w perspektywie nadchodzących lat.

Zapewnienie odporności systemów demokratycznych Unii stanowi część unii bezpieczeństwa: ataki na infrastrukturę wyborczą i systemy informatyczne obsługujące kampanie wyborcze to zagrożenia o charakterze hybrydowym, które wymagają od Unii interwencji. Prowadzenie politycznie motywowanych kampanii dezinformacyjnych w internecie, w tym również przez państwa trzecie, służących dyskredytowaniu i delegitymizacji wyborów, uznano za coraz większe zagrożenie dla naszych demokracji[1]. W ramach swoich uprawnień Unia Europejska powinna podejmować wszelkie działania w celu obrony jej procesów demokratycznych przed manipulacją ze strony państw trzecich lub podmiotów prywatnych. Kampanie wyborcze pokazały, że w czasie, w którym odbywają się wybory, obywatele są szczególnie narażeni na ukierunkowaną dezinformację. Ataki te wpływają na integralność i uczciwość procesu wyborczego oraz na zaufanie obywateli do wybranych przedstawicieli i jako takie zagrażają demokracji.

Obywatele Unii powinni mieć możliwość głosowania z pełnym rozeznaniem w dostępnych alternatywach politycznych. Chodzi również o to, by byli oni świadomi istniejących zagrożeń oraz by życie polityczne było bardziej przejrzyste. Otwarta, bezpieczna sfera publiczna, chroniona przed szkodliwym oddziaływaniem, zapewnia równe warunki prowadzenia

[1] Zob. wspólny komunikat do Parlamentu Europejskiego, Rady Europejskiej i Rady „Zwiększenie odporności i wzmocnienie zdolności reagowania na zagrożenia hybrydowe", JOIN (2018) 16 final oraz konkluzje Rady Europejskiej z dnia 28 czerwca 2018 r. (http://www.consilium.europa.eu/pl/press/press-releases/2018/06/29/20180628-euco-conclusions-final/pdf).

kampanii politycznych i organizowania wyborów, a tym samym zaufanie społeczeństwa[2]. W naszych demokracjach musimy stworzyć przestrzeń do prowadzenia żywej debaty politycznej, która zapewni wyborcom klarowny i niezakłócony obraz idei i programów proponowanych im przez rywalizujące o ich głosy partie polityczne. Dlatego też należy zwalczać oszustwa wyborcze i inne zamierzone próby manipulowania wyborami, w tym poprzez stosowanie sankcji.

Dynamicznie rozwijają się metody wpływania na proces wyborczy za pomocą internetu, zatem kluczowe jest zwiększenie bezpieczeństwa oraz utrzymywanie równych warunków prowadzenia działalności politycznej. Konwencjonalne zabezpieczenia („off-line") stosowane w odniesieniu do wyborów, takie jak przepisy regulujące komunikację polityczną w okresie wyborczym, zapewniające przejrzystość, ograniczenia wydatków na kampanie wyborcze, przestrzeganie ciszy wyborczej oraz równe traktowanie kandydatów, powinny również mieć zastosowanie w internecie[3]. Przejrzystość i ograniczenia dotyczące zamieszczania reklam wyborczych w telewizji lub na billboardach oraz przejrzystość treści reklam politycznych powinny być analogicznie zapewnione w odniesieniu do reklam wyborczych w internecie. Obecnie takich regulacji nie ma, więc należy je wprowadzić przed kolejnymi wyborami do Parlamentu Europejskiego.

Nowe wyzwania i aktualne trendy

Komunikacja z obywatelami przez internet redukuje bariery i koszty dla podmiotów politycznych związane z docieraniem do obywateli oraz wiąże się z ogromnymi możliwościami. Jednocześnie daje ona większe pole do popisu podmiotom działającym w złym zamiarze, które dążą do wywierania wpływu na debatę demokratyczną i procesy wyborcze. Internet może ułatwić podmiotom prezentowanie informacji, jednocześnie umożliwiając im zatajanie źródeł tych informacji lub ich celu, np. poprzez ukrycie, że dany komunikat (np. wpis na portalu społecznościowym) jest płatną reklamą, a nie informacją. To samo dotyczy prezentowania opinii jako informacji lub selektywnego prezentowania informacji w celu wywołania napięć lub polaryzacji debaty. Zagrożeń tych nie należy bagatelizować. Unia Europejska i jej systemy polityczne nie są odporne na tego rodzaju zagrożenia.

[2] Komisja Wenecka Rady Europy wydała wytyczne dotyczące wyborów (http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev-e),dotyczące również środowiska medialnego (http://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2016)006-e).

[3] Zob. niedawno opublikowaną analizę „Internet i kampanie wyborcze – badanie dotyczące wykorzystywania internetu w kampaniach wyborczych" przygotowaną przez komisję ekspertów ds. pluralizmu mediów i przejrzystości stosunków własnościowych w mediach (MSI-MED) przy Radzie Europy (https://www.coe.int/en/web/human-rights-rule-of-law/-/internet-and-electoral-campaigns-a-new-study-has-been-published). W badaniu przeanalizowano konsekwencje przeniesienia reklam wyborczych do internetu, w szczególności w kontekście wydatków i stosowania technik reklamowych w oparciu o tzw. mikrotargetowanie wyborców za pomocą przekazu spersonalizowanego. Zob. również zalecenie Rady Europy CM/Rec(2016)5 w sprawie swobody korzystania z Internetu, które odnosi się do obowiązków rządów, platform i pośredników w zakresie kampanii politycznych prowadzonych przez partie polityczne, kandydatów i inne osoby w internecie.

Ponadto na integralność wyborów mogą niekorzystnie wpływać „konwencjonalne" incydenty cybernetyczne, w tym ataki cybernetyczne ukierunkowane na procesy wyborcze, kampanie, infrastrukturę partii politycznych, systemy obsługujące kandydatów lub organy publiczne oraz niewłaściwe wykorzystywanie danych osobowych. Ostatnie doniesienia, w tym te dotyczące sprawy „Facebook/Cambridge Analytica", są dobrym tego przykładem. Dane osobowe miały zostać wykorzystane niezgodnie z przeznaczeniem i bezprawnie przekazane stronom trzecim w celu odmiennym od tego, który został pierwotnie określony. Doniesienia te zwróciły uwagę na ryzyko związane z pewnymi działaniami podejmowanymi w internecie, polegającymi na kierowaniu do obywateli komunikatów i reklam politycznych, bezprawnym przetwarzaniu i nadużywaniu ich danych osobowych w celu manipulowania poglądami, rozpowszechniania dezinformacji lub po prostu podważania prawdy, o ile służy to celom politycznym lub pogłębia podziały[4].

Wspieranie wolnych i uczciwych wyborów w Europie

Instytucje europejskie nie przeprowadzają wyborów. Podejmowanie działań w tym kontekście należy przede wszystkim do państw członkowskich. Organizowanie wyborów i monitorowanie przebiegu procesu wyborczego to domena państw członkowskich[5]. Niemniej jednak istnieje tutaj oczywisty wymiar unijny. Partie polityczne działające na szczeblu krajowym i regionalnym są głównymi podmiotami w europejskich kampaniach wyborczych, ponieważ wysuwają kandydatów w wyborach do Parlamentu Europejskiego. Europejskie partie polityczne i związane z nimi fundacje odgrywają ważną rolę w organizowaniu dodatkowych kampanii na szczeblu europejskim, w tym kampanii wiodących kandydatów na stanowisko przewodniczącego Komisji Europejskiej.

Po wyborach do Parlamentu Europejskiego w 2014 r. Komisja zobowiązała się w swoim sprawozdaniu powyborczym z 2015 r.[6] do określenia sposobów dalszego wzmacniania wymiaru europejskiego i demokratycznej legitymacji procesu decyzyjnego Unii oraz do dalszego badania przyczyn oraz zaradzenia utrzymującej się niskiej frekwencji w niektórych państwach członkowskich. W lutym 2018 r. Komisja wezwała do jak najszybszego i regularnego angażowania obywateli w debaty dotyczące kwestii europejskich, do tego, by

[4] Zob. sprawozdanie okresowe opublikowane przez brytyjski urząd ochrony danych (ICO) w następstwie wszczęcia formalnego postępowania wyjaśniającego w sprawie wykorzystywania analizy danych do celów politycznych w związku z zarzutami dotyczącymi bezprawnego przetwarzania danych i mikrotargetowania w celu przesyłania reklam politycznych podczas referendum w sprawie pozostania Wielkiej Brytanii w UE lub wyjścia z niej (https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf). W sprawozdaniu podkreślono, że *szybki postęp technologiczny i społeczny w zakresie wykorzystywania dużych zbiorów danych sprawił, że wiedza o stosowanych przez organizacje i przedsiębiorstwa technikach przetwarzania danych (w tym o wykorzystywanych algorytmach, analizach, dopasowywaniu danych i profilowaniu) w celu mikrotargetowania obywateli jest ograniczona lub techniki te są stosowane w sposób mało przejrzysty. Bez wątpienia narzędzia te mogą mieć znaczący wpływ na prywatność obywateli. Istotne jest, aby osiągnąć większą oraz rzeczywistą przejrzystość w zakresie stosowania takich technik po to, by zapewnić obywatelom kontrolę nad ich danymi oraz by nie dochodziło w tym zakresie do obchodzenia prawa. Jeżeli techniki te stosuje się w celu związanym z procesem demokratycznym, wiele argumentów przemawia za tym, aby obowiązywały wysokie standardy przejrzystości*. Podkreśla się również znaczenie kwestii lepszego włączenia problematyki ochrony danych w szersze ramy regulacyjne dotyczące przeprowadzania wyborów.

[5] W ramach prawa UE i ich zobowiązań międzynarodowych.

[6] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Sprawozdanie w sprawie wyborów do Parlamentu Europejskiego w 2014 r. (COM(2015) 206 final).

partie polityczne wcześniej rozpoczęły kampanie wyborcze do Parlamentu Europejskiego, w tym te dotyczące ich kandydatów na stanowisko przewodniczącego Komisji Europejskiej, do zwiększenia przejrzystości w zakresie powiązań między krajowymi i europejskimi partiami politycznymi oraz do promowania przez państwa członkowskie prawa do głosowania, w szczególności w odniesieniu do grup niedostatecznie reprezentowanych.

Unia Europejska również podjęła już pewne ważne kroki w celu budowania odporności demokratycznej w Europie, w tym poprzez ustanowienie nowych europejskich ram ochrony danych, które obowiązują od maja bieżącego roku. Niniejsze ogólne rozporządzenie o ochronie danych, które stało się bezpośrednio stosowane w całej Unii Europejskiej, zapewnia narzędzia niezbędne do przeciwdziałania przypadkom bezprawnego wykorzystywania danych osobowych w kontekście wyborczym. Trwają również prace w celu promowania bezpieczniejszego środowiska internetowego poprzez zwiększenie ogólnej odporności na zagrożenia cybernetyczne, w tym stosowanie dezinformacji i manipulacji behawioralnej w internecie.

Istotne jest, abyśmy osiągnęli jak największą jasność co do sposobu wdrażania europejskich przepisów o ochronie danych w tym nowym kontekście. Jednocześnie musimy zwiększyć wysiłki na rzecz poprawy świadomości, przejrzystości i bezpieczeństwa. Obywatele powinni móc identyfikować nadawców internetowych reklam i komunikatów politycznych oraz zleceniodawców tych treści. Wytyczne dotyczące wdrażania nowych przepisów o ochronie danych w kontekście wyborów europejskich powinny przyczynić się do większej przejrzystości i świadomości w tym zakresie, jako że ściślejsza współpraca i wymiana informacji między właściwymi organami oraz z innymi podmiotami przyczyniają się do zwiększenia bezpieczeństwa.

Przedstawiony wraz z niniejszym komunikatem pakiet na rzecz wzmocnienia odporności demokratycznej obejmuje zrównoważone, kompleksowe i ukierunkowane działania służące przeprowadzeniu w sposób efektywny i uczciwy wyborów do Parlamentu Europejskiego w 2019 r. Jest to wspólny obowiązek wszystkich podmiotów uczestniczących w procesie wyborczym. Wymaga to ciągłej czujności oraz elastycznego dostosowywania się do zmiennego otoczenia i nowych osiągnięć technologicznych. Dzięki opracowaniu wytycznych, zaleceń i niezbędnych narzędzi krajowe i europejskie partie polityczne, rządy państw, organy, podmioty prywatne i zainteresowane strony będą mogły współpracować z większą przejrzystością przy kreowaniu bezpieczniejszego otoczenia demokratycznego oraz na równych warunkach działania.

Zachęca się również państwa członkowskie do stosowania tych zasad do innych wyborów i referendów organizowanych na szczeblu krajowym.

Proponowane w ramach tego pakietu środki mają na celu:

1. dostarczenie szczegółowych wytycznych dotyczących przetwarzania danych osobowych na potrzeby wyborów;

2. zalecenie najlepszych praktyk w zakresie przeciwdziałania zagrożeniom związanym z dezinformacją i atakami cybernetycznymi oraz promowanie przejrzystości i rozliczalności w internecie w procesie wyborczym UE; oraz wzmocnienie współpracy między właściwymi organami i dostarczenie narzędzi umożliwiających podejmowanie interwencji, a w razie konieczności zastosowanie sankcji w celu ochrony integralności wyborów.
3. Reagowanie na przypadki czerpania przez partie polityczne lub związane z nimi fundacje korzyści z praktyk naruszających przepisy o ochronie danych, z zamiarem wpływania lub usiłowania wywarcia wpływu na wyniki wyborów europejskich.

Przedstawiając ten pakiet, Komisja zadbała o to, by uniknąć niepotrzebnych obciążeń administracyjnych oraz niewłaściwego ograniczenia swobody europejskich, regionalnych i krajowych partii i fundacji politycznych.

1. Aktualnie stosowane przez UE środki służące zapewnieniu wolnych i uczciwych wyborów

Unia podjęła już zdecydowane kroki w celu ochrony integralności wyborów i wzmocnienia procesu demokratycznego.

Zgodnie z ogólnym rozporządzeniem o ochronie danych,[7] które jest bezpośrednio stosowane w całej Unii od dnia 25 maja 2018 r. Unia Europejska jest obecnie w pełni wyposażona, aby udzielać wsparcia w zapobieganiu przypadkom bezprawnego wykorzystywania danych osobowych. Unia Europejska wyznacza standardy w tym obszarze.

Ponadto niedawno zmieniono akt dotyczący wyborów posłów do Parlamentu Europejskiego, by m.in. zapewnić jeszcze więcej przejrzystości w europejskim procesie wyborczym[8]. Zmienione rozporządzenie w sprawie statutu i finansowania europejskich partii politycznych[9], które zostało przyjęte w dniu 3 maja 2018 r., zwiększa identyfikację, skuteczność, przejrzystość i rozliczalność działalności europejskich partii politycznych i europejskich fundacji politycznych. W zaleceniu Komisji (UE) 2018/234[10] podkreślono kluczowe działania mające na celu dalsze usprawnienie procesu wyborów do Parlamentu Europejskiego w 2019 r.

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).
[8] Decyzja Rady (UE, Euratom) 2018/994 z dnia 13 lipca 2018 r. zmieniająca Akt dotyczący wyborów członków Parlamentu Europejskiego w powszechnych wyborach bezpośrednich, załączony do decyzji Rady 76/787/EWWiS, EWG, Euratom z dnia 20 września 1976 r.(https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX:32018D0994&qid=1531826494620).
[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 1141/2014 z dnia 22 października 2014 r. w sprawie statusu i finansowania europejskich partii politycznych i europejskich fundacji politycznych (Dz.U. L 317 z 4.11.2014, s. 1).
[10] Zalecenie Komisji (UE) 2018/234 z dnia 14 lutego 2018 r. w sprawie uwydatnienia europejskiego charakteru i usprawnienia procesu wyborów do Parlamentu Europejskiego w 2019 r. (Dz.U. L 45 z 17.2.2018, s. 40)

Dyrektywę Parlamentu Europejskiego i Rady 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej[11]) stosuje się do niezamówionych komunikatów do celów marketingu bezpośredniego, w tym komunikatów politycznych przekazywanych przez partie polityczne i inne podmioty zaangażowane w proces polityczny. Zapewnia również poufność i ochronę informacji przechowywanych w urządzeniach końcowych użytkownika, takich jak smartfon czy komputer[12]. Proponowane rozporządzenie w sprawie prywatności i łączności elektronicznej,[13] które jest obecnie przedmiotem negocjacji, wzmocni kontrolę obywatelską dzięki zwiększeniu przejrzystości i rozszerzeniu zakresu ochrony ponad tradycyjnych operatorów telekomunikacyjnych, tak aby swoim zasięgiem objąć internetowe usługi komunikacji elektronicznej.

Ponadto w swoim komunikacie z dnia 26 kwietnia 2018 r.[14] Komisja przedstawiła również europejskie podejście do kwestii dezinformacji w internecie. W niniejszym komunikacie Komisja pragnie wspierać tworzenie bardziej przejrzystej, wiarygodnej i rozliczalnej sieci internetowej. Jednym z kluczowych jej celów jest opracowanie ambitnego **kodeksu postępowania w zakresie zwalczania dezinformacji** który w szczególności powinien objąć platformy internetowe i branżę reklamową, aby zapewnić przejrzystość oraz ograniczyć możliwości celowego dobierania odbiorców (targeting) reklam politycznych.[15] Przewiduje się, że kodeks zostanie opublikowany we wrześniu 2018 r.[16]. Powinien on przynieść wymierne rezultaty do października.

Ściślej rzecz ujmując, sygnatariusze kodeksu postępowania powinni zgodzić się, że oszukańcze strony internetowe oraz zawierające treści dezinformujące będą pozbawione dochodów z reklam. Powinni oni również zapewnić przejrzystość sponsorowanych treści, w szczególności reklamy politycznej i tematycznej, ustanowić jasne systemy znakowania i zasady dotyczące botów,[17] aby wykluczyć podobieństwo ich działania z interakcjami ludzkimi. Należy również zintensyfikować wysiłki na rzecz zamykania fałszywych kont. Sygnatariusze powinni także zgodzić się na wprowadzenie dla użytkowników ułatwień w zakresie oceny treści, poprzez wsparcie dla tworzenia wskaźników oceny wiarygodności źródeł, z których te treści pochodzą. Powinni oni również uzgodnić zmniejszenie widoczności dezinformacji poprzez ułatwienie wyszukiwania wiarygodnych treści oraz dostarczenie

[11] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

[12] Strony internetowe mogą uzyskać dostęp do takich informacji lub śledzić zachowania użytkownika w sieci, np. za pomocą przechowywanych na urządzeniu użytkownika plików cookies, za uprzednią jego zgodą.

[13] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), COM(2017)10 final.

[14] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów. Zwalczanie dezinformacji w internecie: podejście europejskie (COM (2018) 236 final).

[15] W celu przygotowania tego kodeksu Komisja zwołała w maju 2018 r. forum, które podzielono na „grupę roboczą" (w skład której wchodzą główne platformy internetowe i przedstawiciele branży reklamowej oraz główni reklamodawcy) oraz „radę konsultacyjną" (składającą się z przedstawicieli mediów i społeczeństwa obywatelskiego).

[16] Po wydaniu opinii przez radę konsultacyjną.

[17] Boty wykorzystuje się m. in. do zamieszczania w sposób zautomatyzowany wpisów na platformach społecznościowych oraz do bardziej interaktywnych zastosowań, jak np. chatboty, które bezpośrednio komunikują się z użytkownikami.

użytkownikom informacji o priorytetyzacji treści za pomocą algorytmów. Ponadto sygnatariusze powinni zapewnić organizacjom, które są zaufanymi podmiotami weryfikującymi informacje, oraz środowisku akademickiemu dostęp do danych będących w posiadaniu platform. Ocena kodeksu postępowania będzie częścią prac nad planem działania zawierającym szczegółowe wnioski dotyczące skoordynowanej reakcji UE na problem dezinformacji. Komisja i wysoki przedstawiciel przedstawią ją przed końcem roku.

Jeżeli chodzi o bardziej „tradycyjne" cyberincydenty, takie jak włamania do systemów informatycznych lub ataki polegające na podmianie treści stron internetowych, definicje przestępstw oraz granice dolna i górna zagrożenia karą w zakresie ataków na systemy informatyczne zostały zharmonizowane na poziomie Unii Europejskiej dyrektywą 2013/40/UE dotyczącej ataków na systemy informatyczne.

Grupa współpracy ustanowiona na mocy dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148[18] stwierdziła, że bezpieczeństwo cybernetyczne wyborów to wspólne wyzwanie. Grupa współpracy, złożona z krajowych organów właściwych ds. bezpieczeństwa cybernetycznego, Komisji oraz Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji („ENISA"), określiła krajowe inicjatywy w zakresie bezpieczeństwa cybernetycznego sieci oraz systemów informatycznych wykorzystywanych w wyborach. Zidentyfikowała ona zagrożenia związane z niewystarczającym poziomem bezpieczeństwa cybernetycznego mogące wywierać wpływ na kolejne wybory do Parlamentu Europejskiego oraz opracowała kompendium dotyczące bezpieczeństwa cybernetycznego technologii wyborczych, obejmujące środki techniczne i organizacyjne oparte na doświadczeniach i najlepszych praktykach. Kompendium zawiera wskazówki praktyczne dla organów ds. bezpieczeństwa cybernetycznego i organów zarządzających wyborami.

2. Dalsze wzmacnianie odporności demokratycznej: wzmocnienie sieci współpracy, przejrzystość w internecie, ochrona przed cyberincydentami oraz zwalczanie z kampanii dezinformacyjnych w kontekście wyborów do Parlamentu Europejskiego

Biorąc pod uwagę skalę wyzwań oraz fakt, że zadania i obowiązki w tym obszarze formalnie podzielone są między wiele organów, namacalne rezultaty zostaną osiągnięte jedynie wówczas, gdy dojdzie do współdziałania wszystkich właściwych podmiotów.

Niniejszemu komunikatowi towarzyszy zalecenie w sprawie sieci współpracy wyborczej, przejrzystości w internecie, ochrony przed cyberincydentami i zwalczania kampanii dezinformacyjnych w kontekście wyborów do Parlamentu Europejskiego. Aby zapewnić wolne i uczciwe wybory, niniejsze zalecenie powinno zostać wdrożone przez wszystkie

[18] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

podmioty z odpowiednim wyprzedzeniem w perspektywie wyborów do Parlamentu Europejskiego w 2019 r.

W zaleceniu zachęcamy wszystkie państwa członkowskie do utworzenia i wspierania krajowej sieci wyborczej. Organy państw członkowskich właściwe ds. wyborów powinny sprawnie i efektywnie współpracować z organami właściwymi w obszarach powiązanych (takich jak organy ochrony danych, regulatorzy mediów, organy ds. bezpieczeństwa cybernetycznego itp.). W razie potrzeby organy te powinny również współdziałać z organami ścigania. Umożliwi im to szybkie wykrywanie potencjalnych zagrożeń dla wyborów do Parlamentu Europejskiego oraz sprawne egzekwowanie obowiązujących przepisów, w tym stosowanie dostępnych sankcji finansowych, takich jak nakaz zwrotu wkładu publicznego. Należy przestrzegać przepisów unijnych i krajowych oraz egzekwować je. W tym kontekście Komisja wzywa państwa członkowskie do wspierania, zgodnie z odpowiednimi przepisami krajowymi i unijnymi, wymiany informacji pomiędzy organami ochrony danych a organami właściwymi ds. monitorowania wyborów oraz monitorowania działalności partii politycznych i finansowania ich, jeżeli z ich decyzji wynika lub gdy istnieją uzasadnione podstawy, by sądzić, że dane naruszenie wiąże się z działalnością polityczną krajowych partii politycznych lub fundacji w kontekście wyborów do Parlamentu Europejskiego.

Zaleca się również, by państwa członkowskie wyznaczyły punkty kontaktowe uczestniczące w europejskiej sieci współpracy na potrzeby wyborów do Parlamentu Europejskiego. Komisja udzieli wsparcia tym sieciom współpracy, organizując pierwsze posiedzenie wyznaczonych punktów kontaktowych do stycznia 2019 r. Z poszanowaniem kompetencji krajowych i wymogów proceduralnych mających zastosowanie do zainteresowanych organów, forum to będzie stanowić rdzeń europejskiego procesu ostrzegania w czasie rzeczywistym oraz będzie miejscem wymiany informacji i praktyk pomiędzy organami państw członkowskich.

Partie polityczne, fundacje i organizacje kampanijne powinny zagwarantować stosowanie przejrzystych praktyk w komunikacji politycznej z obywatelami oraz zapewnić, aby europejski proces wyborczy nie był zakłócany przez nieuczciwe praktyki. Komisja przedstawia konkretne środki mające na celu zwiększenie przejrzystości, tak aby obywatel mógł zidentyfikować zarówno autora danego komunikatu politycznego, który otrzymał, jak i jego zleceniodawcę[19]. Państwa członkowskie powinny wspierać i ułatwiać taką przejrzystość oraz wysiłki właściwych organów w zakresie monitorowania naruszeń i egzekwowania przepisów, w tym poprzez stosowanie sankcji tam, gdzie to konieczne. W stosownych przypadkach organy ścigania powinny również działać w celu zapewnienia adekwatnej reakcji na incydenty i zastosowania odpowiednich sankcji[20].

[19] Propozycje te uzupełniają kodeks postepowania opracowywany przez wielostronne forum zwołane przez Komisję po wydaniu komunikatu z dnia 26 kwietnia 2018 r. w sprawie dezinformacji w internecie.

[20] Kwestia ta dotyczyłaby w szczególności przypadków, w których proces wyborczy jest przedmiotem oddziaływania w złych zamiarach, w tym wywołania incydentów polegających na atakach na systemy informatyczne. W zależności od okoliczności właściwe może być przeprowadzenie postępowania karnego, które może zakończyć się nałożeniem sankcji

Odporność, prewencja i obrona stanowią fundament dla budowy silnego systemu bezpieczeństwa cybernetycznego Unii Europejskiej[21]. Właściwe organy europejskie i krajowe, partie polityczne, fundacje i organizacje kampanijne powinny być w pełni świadome zagrożeń związanych z wyborami, które odbędą się w przyszłym roku, i podejmować odpowiednie wysiłki, aby chronić ich sieci i systemy informatyczne[22].

3. Stosowanie przepisów o ochronie danych w procesie wyborczym

Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady (ogólne rozporządzenie o ochronie danych)[23], które jest bezpośrednio stosowane w całej Unii od dnia 25 maja 2018 r., zapewnia Unii narzędzia niezbędne do przeciwdziałania przypadkom bezprawnego wykorzystywania danych osobowych w kontekście wyborczym.

Ponieważ po raz pierwszy przepisy te będą stosowane w kontekście wyborów europejskich, przy okazji zbliżających się wyborów do Parlamentu Europejskiego, istotne jest, aby wszystkie podmioty biorące udział w procesach wyborczych – takie jak krajowe organy wyborcze, partie polityczne, pośrednicy i analitycy danych, platformy społecznościowe oraz sieci reklam internetowych – jednoznacznie rozumiały, w jaki sposób najlepiej stosować te przepisy oraz co na ich podstawie jest dozwolone i niedozwolone.

W związku z tym Komisja przygotowała szczegółowe wytyczne w celu podkreślenia obowiązków w zakresie ochrony danych, które mają znaczenie w kontekście wyborczym. Aby zwalczać podejmowane w złym zamiarze próby nadużycia danych osobowych obywateli, w szczególności do celów mikrotargetowania, krajowe organy ochrony danych, jako organy egzekwujące ogólne rozporządzenie o ochronie danych, mają obowiązek w pełni wykorzystać swoje zwiększone uprawnienia w celu przeciwdziałania ewentualnym naruszeniom.

---

karnych. Jak wskazano powyżej, definicje przestępstw oraz górna i dolna granica zagrożenia karą za przeprowadzenie ataków na system informatyczny zostały ujednolicone dyrektywą 2013/40/UE.

[21] Wspólny komunikat Wysokiej Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa oraz Komisji Europejskiej z września 2017 r. potwierdza potrzebę podjęcia kompleksowych działań w celu stworzenia silnego systemu bezpieczeństwa cybernetycznego w Unii, opartego na odporności, prewencji i obronie, JOIN (2017) 450 final.

[22] Kompendium opracowane przez grupę współpracy ustanowioną na mocy dyrektywy (UE) 2016/1148 zawiera przydatne wskazówki w tym zakresie. Celem dyrektywy (UE) 2016/1148 jest osiągnięcie wysokiego wspólnego poziomu odporności w zakresie bezpieczeństwa cybernetycznego w całej Unii. Aby osiągnąć ten cel, dyrektywa wspiera rozwijanie krajowych zdolności w zakresie bezpieczeństwa cybernetycznego oraz chroni świadczenie podstawowych usług w kluczowych sektorach. W celu wzmocnienia wysiłków na rzecz prawidłowego wdrożenia dyrektywy do 2020 r. Komisja zapewnia finansowanie w wysokości ponad 50 mln EUR w ramach instrumentu „Łącząc Europę". Środki zarządzania ryzykiem przewidziane w dyrektywie (UE) 2016/1148 są odpowiednimi wskaźnikami referencyjnymi w odniesieniu do procesu wyborczego. W ogólnym rozporządzeniu o ochronie danych przewidziano również obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa przetwarzanych danych osobowych. Ma ono zastosowanie do wszystkich podmiotów uczestniczących w procesie wyborczym, a także nakłada obowiązek zgłaszania właściwym organom ochrony danych oraz zainteresowanym osobom naruszeń danych osobowych (zob. wytyczne wydane przez Komisję).

[23] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

4. Wzmocnienie przepisów o finansowaniu europejskich partii politycznych

Co oczywiste, partie polityczne i fundacje odgrywają kluczową rolę w wyborach. Konkurują one o głosy wyborców w ramach swoich kampanii. Aby zapewnić równe warunki działania na poziomie politycznym oraz chronić wszystkie partie polityczne i fundacje przed nadużyciami niezbędne jest zapobieganie sytuacjom, w których jakakolwiek partia może odnieść korzyści z nielegalnych praktyk naruszających przepisy w zakresie ochrony danych. Te z nich, które nie tylko naruszają prywatność obywateli, ale również potencjalnie mogłyby wpłynąć na wyniki wyborów do Parlamentu Europejskiego, powinny podlegać sankcjom. Oprócz wezwania państw członkowskich do stosowania, jeżeli to konieczne, takich sankcji wobec partii i fundacji na szczeblu krajowym, Komisja proponuje wprowadzenie ukierunkowanej zmiany w rozporządzeniu (UE, Euratom) nr 1141/2014 w celu zapewnienia proporcjonalnych sankcji w sprawach z udziałem partii i fundacji politycznych na szczeblu europejskim. Nowelizacja ta, która wzmacnia obowiązujące przepisy, ma na celu zapewnienie, aby wybory do Parlamentu Europejskiego mogły odbywać się na zasadach ściśle demokratycznych oraz przy pełnym poszanowaniu wartości, na których opiera się Unia, w szczególności demokracji, praw podstawowych i praworządności.

Komisja apeluje do Parlamentu Europejskiego i Rady o zapewnienie, aby te zmiany zostały przyjęte przed wyborami do Parlamentu Europejskiego w 2019 r.

5. Podsumowanie

Ostatnie wydarzenia pokazały, że ryzyko manipulowania procesem wyborczym, czy to poprzez ataki na systemy informatyczne, nielegalne wykorzystywanie danych osobowych oraz stosowanie nieprzejrzystych praktyk, jest realne i poważne. UE nie jest na nie odporna. Aktywność w internecie w okresie wyborczym stanowi nowe zagrożenie, które wymaga zastosowania szczególnych środków ochrony. Najlepszy sposób, w jaki służymy obywatelom i demokracji, to bycie przygotowanymi. Nie możemy czekać aż do zakończenia wyborów lub referendum, by się o tych incydentach dowiedzieć i dopiero wtedy na nie zareagować.

Ochrona demokracji w Unii to wspólny obowiązek Unii Europejskiej i jej państw członkowskich. Jest to również problem wymagający niezwłocznych działań. Wszystkie zaangażowane podmioty muszą zintensyfikować swoje wysiłki i współdziałać w celu powstrzymywania celowego zakłócania systemu wyborczego, zapobiegania mu i stosowania odpowiednich sankcji. Środki zaproponowane przez Komisję w ramach tego pakietu wspierają owe wysiłki.

Po wyborach europejskich w 2019 r. Komisja przedstawi Parlamentowi Europejskiemu sprawozdanie z wdrożenia tego pakietu środków.

Kolejne kroki przed wyborami do Parlamentu Europejskiego w 2019 r.

- *Komisja apeluje do Parlamentu Europejskiego i Rady o terminowe przyjęcie proponowanych zmian w rozporządzeniu (UE, Euratom) nr 1141/2014 przed wyborami do Parlamentu Europejskiego w 2019 r.*

- *Wspólnie z wysoką przedstawiciel Komisja będzie wspierać przygotowanie wspólnych europejskich reakcji na każdą zewnętrzną ingerencję w wybory w Unii Europejskiej*[24]*. W następstwie konkluzji Rady Europejskiej z czerwca 2018 r., w grudniu 2018 r., we współpracy z państwami członkowskimi, przedstawiony zostanie plan działania dotyczący skoordynowanej reakcji UE na problem dezinformacji.*

- *Komisja podniesie poziom świadomości i utrzyma dialog z władzami państw członkowskich za pośrednictwem konferencji wysokiego szczebla w sprawie zagrożeń cybernetycznych, która odbędzie się w dniach 15–16 października 2018 r. Jej rezultaty zostaną uwzględnione podczas kolejnego sympozjum na temat praw podstawowych (w dniach 26–27 listopada 2018 r.), które poświęcone będzie „Demokracji w Unii Europejskiej”.*

[24] Może on również obejmować stosowanie środków opracowanych w zakresie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne.