



ORĘDZIE O STANIE UNII 2018



Wolne i uczciwe wybory europejskie

#SOTEU

12 września 2018 r.

„Chcę, aby obywatele Europy mogli dokonać wyborów politycznych w maju przyszłego roku podczas uczciwych, bezpiecznych i przejrzystych wyborów europejskich. Ryzyko ingerencji i manipulacji w naszej przestrzeni internetowej nigdy nie było tak wysokie. Czas dostosować nasze zasady wyborcze do tempa rozwoju epoki cyfrowej, aby chronić demokrację europejską”.

Jean-Claude Juncker, 12 września 2018 r.



Jednym z elementów unii bezpieczeństwa jest zapewnienie odporności systemów demokratycznych Unii. Dlatego też przewodniczący Jean-Claude Juncker przedstawił w swoim orędziu o stanie Unii konkretne środki służące temu, aby przyszłoroczne **wybory** do Parlamentu Europejskiego przebiegły w sposób **wolny, sprawiedliwy i bezpieczny**. Komisja przedstawia dzisiaj potencjalne zagrożenia dla przebiegu wyborów i proponuje rozwiązania, jakie rządy i władze krajowe, partie polityczne, media i platformy cyfrowe mogą zastosować, aby sobie z nimi poradzić.

Zaproponowane środki obejmują:

- zalecenie w sprawie sieci współpracy wyborczej, przejrzystości w internecie, ochrony przed cyberincydentami i zwalczania kampanii dezinformacyjnych;
- wytyczne dotyczące stosowania ogólnego rozporządzenia UE o ochronie danych;
- zaostrzenie przepisów dotyczących finansowania europejskich partii politycznych.



Środki mające na celu ochronę wyborów europejskich skupiają się na następujących aspektach:

OCHRONA DANYCH: zapewnienie lepszej ochrony danych osobowych w kontekście wyborczym

PRZEJRZYŚĆ: zapewnienie przejrzystości reklam politycznych umieszczanych w internecie

CYBERBEZPIECZEŃSTWO: ochrona wyborów przed cyberatakami

WSPÓŁPRACA: zapewnienie lepszej krajowej i europejskiej współpracy w zakresie potencjalnych zagrożeń dla wyborów do Parlamentu Europejskiego

WŁAŚCIWE SANKCJE: zapewnienie powszechnego poszanowania zasad wyborczych



OCHRONA DANYCH

Niedawne doniesienia, w tym w związku ze sprawą „Facebook/Cambridge Analytica”, w której najwyraźniej doszło do wykorzystania danych osobowych w niewłaściwy sposób, zwróciły uwagę na ryzyko związane z niektórymi działaniami w internecie w kontekście procesu wyborczego.

Komisja opracowała **wytyczne** na użytek europejskich partii politycznych, fundacji, krajowych organów wyborczych, a także platform mediów społecznościowych, objaśniając, **w jaki sposób należy stosować nowe unijne ogólne rozporządzenie o ochronie danych (RODO), mające zastosowanie od maja 2018 r., w kontekście wyborów.**



PRZEJRZYSTOŚĆ

Podczas gdy w rzeczywistości niewirtualnej przy organizacji wyborów należy stosować się do pewnych wymogów i zasad, takich jak przejrzystość i limity wydatków na kampanie wyborcze, okresy ciszy wyborczej oraz równe traktowanie kandydatów przez media w trakcie kampanii wyborczej, bardzo łatwo obejść te wymagania w internecie.

Komisja rozpoczęła już prace nad kwestią dezinformacji w internecie. Kodeks praktyk powinien zobowiązać platformy internetowe i branżę reklamową do zapewnienia przejrzystości i ograniczenia opcji celowego dobierania odbiorców (targeting) reklam politycznych. Kodeks ma zostać zatwierdzony do końca września 2018 r. Komisja będzie uważnie śledzić proces, oceniać postępy i analizować pierwsze wyniki wdrożenia kodeksu praktyk przed końcem 2018 r.

Komisja przedstawia zalecenia dla władz oraz partii politycznych i fundacji w państwach UE dotyczące sposobów **zapewnienia przejrzystości reklam politycznych:**



Partie polityczne, fundacje i organizacje biorące udział w kampanii powinny udostępniać obywatelom informacje o tym, ile pieniędzy przeznaczają w trakcie swojej kampanii na reklamę w internecie.



Powinny one wyraźnie wskazywać, która partia lub polityczna grupa wsparcia stoi za daną płatną reklamą polityczną umieszczaną w internecie.



Powinny też przekazywać obywatelom europejskim informacje o tym, w jaki sposób dobierani są adresaci takich reklam.



W przypadku niezastosowania się do tych zasad państwa członkowskie powinny nałożyć odpowiednie sankcje wyborcze.



WSPÓŁPRACA KRAJOWA I EUROPEJSKA

Współpraca na szczeblu krajowym i unijnym między różnymi podmiotami zaangażowanymi w proces wyborczy pomoże w wykrywaniu potencjalnych zagrożeń (w tym również hybrydowych) dla przebiegu wyborów i szybkim rozwiązywaniu tych problemów.

W kwietniu 2018 r. Komisja zorganizowała pierwszą wymianę między krajami UE dotyczącą najlepszych praktyk wyborczych. W ramach działań następczych i w perspektywie wyborów do Parlamentu Europejskiego w 2019 r. Komisja ustanowi europejską sieć współpracy. Dwa dodatkowe spotkania zostaną zorganizowane w styczniu i kwietniu 2019 r.

Komisja zaleca, aby władze państw UE poprawiły:

- ▶ **współpracę na szczeblu krajowym** – każde państwo powinno wyznaczyć krajową sieć współpracy w dziedzinie wyborów, która koordynować będzie działania różnych krajowych organów (organów właściwych w sprawach wyborczych oraz organów odpowiedzialnych za monitorowanie i egzekwowanie przepisów dotyczących działalności w internecie). Umożliwi im to szybkie wykrycie potencjalnych zagrożeń dla przebiegu wyborów do Parlamentu Europejskiego oraz sprawne egzekwowanie istniejących przepisów, w tym poprzez stosowanie sankcji;
- ▶ **współpracę na szczeblu europejskim** – każde państwo powinno wyznaczyć pojedynczy punkt kontaktowy do celów wdrożenia zalecenia. Ułatwi to wymianę wiedzy fachowej i najlepszych praktyk między państwami UE, w tym w zakresie zagrożeń, luk i egzekwowania prawa.



CYBERBEZPIECZEŃSTWO

Ataki cybernetyczne stanowią zagrożenie dla wyborów, kampanii, partii politycznych, kandydatów oraz organów władzy publicznej i mogą mieć wpływ na uczciwość i sprawiedliwość procesu wyborczego.

Wraz z organami krajowymi odpowiedzialnymi za bezpieczeństwo cybernetyczne oraz Agencją Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) Komisja opracowała kompendium zawierające szczegółowe wytyczne dotyczące zagrożeń dla bezpieczeństwa cybernetycznego. Jednocześnie z zaleceniem Komisja proponuje utworzenie sieci centrów kompetencji w dziedzinie cyberbezpieczeństwa oraz nowego europejskiego centrum kompetencji, aby lepiej ukierunkować i koordynować dostępne środki finansowe na współpracę w dziedzinie cyberbezpieczeństwa, badań naukowych i innowacji.

Komisja zaleca, aby:

- ▶ władze w państwach UE przyjęły środki techniczne i organizacyjne **w celu zarządzania zagrożeniami dla bezpieczeństwa sieci i systemów informatycznych** wykorzystywanych przy organizacji wyborów do Parlamentu Europejskiego;
- ▶ organy krajowe państw członkowskich odpowiedzialne za bezpieczeństwo cybernetyczne stosowały opracowane wytyczne dotyczące zagrożeń dla bezpieczeństwa cybernetycznego.



WŁAŚCIWE SANKCJE

Komisja proponuje **wprowadzenie kar finansowych w wysokości 5% rocznego budżetu europejskiej partii politycznej lub fundacji** nakładanych w przypadku naruszenia przez nie przepisów o ochronie danych osobowych w celu wywierania wpływu na wynik wyborów do Parlamentu Europejskiego. Ukarana partia lub fundacja nie mogłaby ponadto składać wniosku o finansowanie z budżetu ogólnego Unii Europejskiej w roku, w którym nałożono na nią karę. Przepisy te będą egzekwowane przez Urząd ds. Europejskich Partii Politycznych i Europejskich Fundacji Politycznych. W odniesieniu do reklam politycznych władze państw członkowskich powinny stosować właściwe sankcje wyborcze w przypadku nieprzestrzegania zasad przejrzystości.

