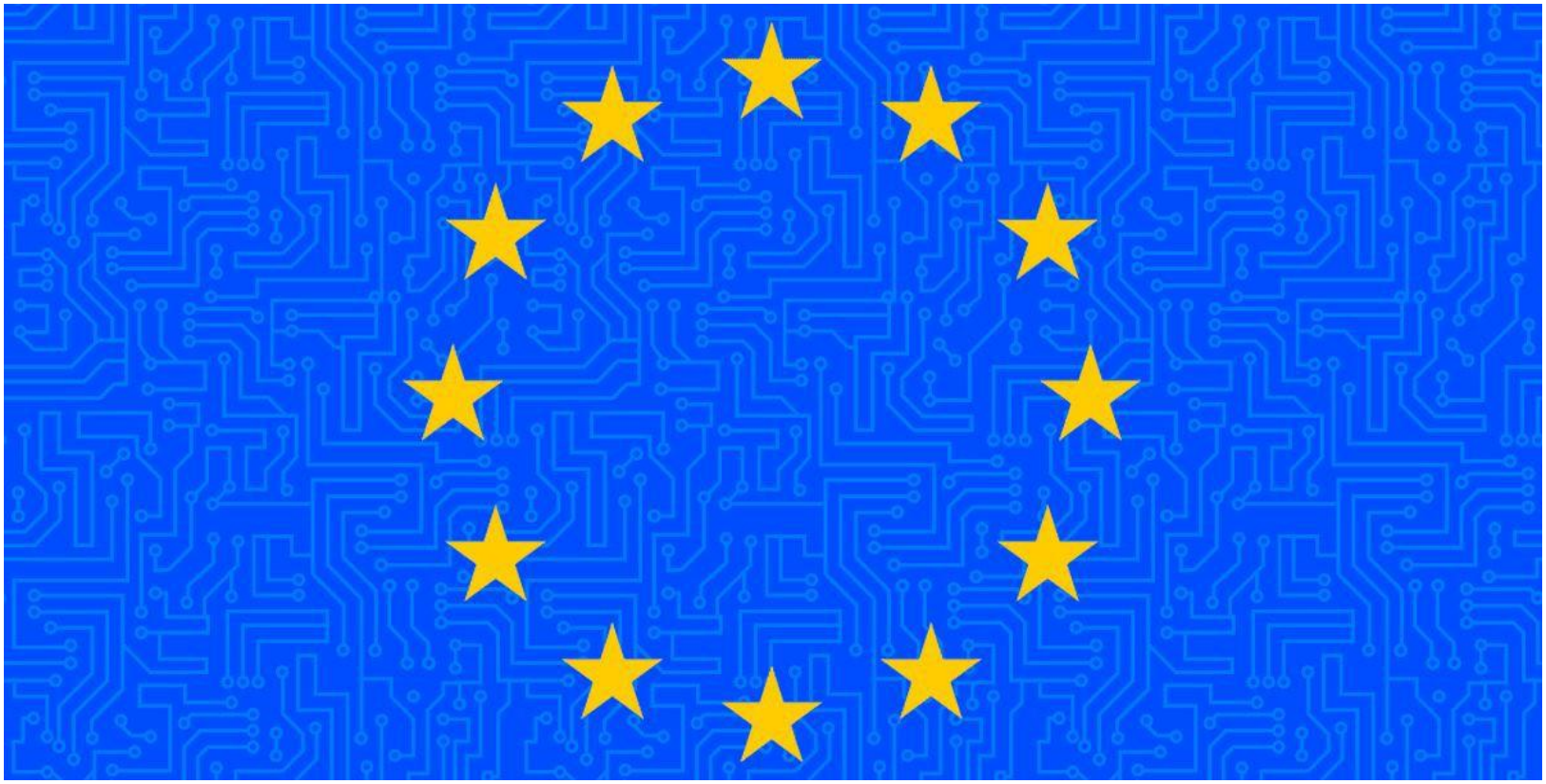

Należy zachować to, co sprawnie działa i naprawić to, co nie działa lub zostało zepsute:

Zasady programowe EFF dotyczące ustawy o usługach cyfrowych

ELECTRONIC FRONTIER FOUNDATION

Opublikowano w 2020 r.
Publikacja Electronic Frontier Foundation z 2020 r. „Należy zachować to, co sprawnie działa i naprawić to, co nie działa lub zostało zepsute: Zasady programowe EFF dotyczące ustawy o usługach cyfrowych” wydana na podstawie międzynarodowej licencji Creative Commons Attribution 4.0 (CC BY 4.0).

Kontakt
Christoph Schmon, dyrektor ds. polityki międzynarodowej:
christoph@eff.org Zapytania ze strony mediów: press@eff.org

Unijny rejestr przejrzystości
805637038375-01

Treść

Należy zachować to, co sprawnie działa i naprawić to, co nie działa lub zostało zepsute

Internet widział lepsze dni. Kiedyś obiecywał wyzwolenie: każdy z urządzeniem komputerowym może połączyć się ze światem, anonimowo lub nieanonimowo, żeby opowiedzieć swoją historię, załatwić swoje sprawy, kształcić i uczyć się. Dzisiaj jednak dla wielu z nas doświadczenie online oznacza bycie zamkniętym w ramach kilku potężnych platform i cały czas bez naszej zgody śledzonym w Internecie. A możliwość uzyskiwania dostępu i dzielenia się informacjami pozostaje na łasce algorytmicznych systemów decyzyjnych, które zarządzają naszym życiem online. Strasznie ucierpiały podstawowe zasady, takie jak przejrzystość, otwartość i samostanowienie informacyjne, które kiedyś w czasach wczesnego Internetu odgrywały kluczową rolę.

Procesy te jednak nie są oraz nie muszą być nieuniknione i trwałe. Bowiem to do nas należy kształtowanie Internetu, a jego ostateczna forma będzie częściowo zależała od rzetelnego przeglądu obowiązujących przepisów technologicznych, z uwzględnieniem gospodarki platform XXI wieku. Możemy ulepszyć to, co już istnieje, lecz musimy jednocześnie zabezpieczyć elementy obecnego porządku prawnego, które działają sprawnie.

W Unii Europejskiej powstaje szansa, żeby właśnie to zrobić: przyjąć przyszłościowe regulacje pozwalające zachować zasady, które inspirowały innowacje i chroniły prawa podstawowe, jednocześnie wzmacniając pozycję użytkowników i przyszłych innowatorów. W 2020 r. Komisja Europejska ogłosiła ambitną strategię promowania wyraźnie odrębnej europejskiej wizji regulacji działalności dużych firm technologicznych. Częścią tej strategii jest pakiet ustawy o usługach cyfrowych. Ustawa o usługach cyfrowych (DSA) jest najważniejszą reformą europejskiego prawodawstwa dotyczącego działalności platform, czyli dyrektywy o handlu elektronicznym, jaką UE podjęła od dwudziestu lat. Reforma stanowi niepowtarzalną okazję do sformułowania odważnej, opartej na dowodach wizji sprostania najpilniejszym wyzwaniom dzisiejszych czasów.

Popieramy zaangażowanie Komisji na rzecz lepszej alternatywnej przyszłości Internetu i z zadowoleniem przyjmujemy wyrażaną przez Komisję ambicję znalezienia kreatywnych rozwiązań złożonych kwestii, takich jak problematyka przejrzystości, prywatyzacja moderacji treści i rynki zdominowane przez strażników. Uczestniczyliśmy w przygotowaniu sprawozdań dla Parlamentu Europejskiego i w konsultacjach Komisji w sprawie DSA. Będziemy nadal ściśle współpracować z instytucjami UE, żeby dzielić się naszymi doświadczeniami w walce o prawa cyfrowe w drodze postępowań sądowych prowadzących do kształtowania zmian społecznych, oddolnego aktywizmu i rozwoju technologii.

Jesteśmy też ostrożni. Najnowsze przepisy, takie jak dyrektywa o prawach autorskich oraz inicjatywy regulacyjne w Niemczech, Francji i Austrii , które próbują rozwiązywać podobne problemy, zagrażają wolności wypowiedzi w Internecie, a jednocześnie przyznają prywatnym platformom jeszcze większą odpowiedzialność i obowiązki w zakresie kontroli treści użytkowników. Ustawa DSA jest istotnym przyczynkiem do potwierdzenia zaangażowania UE na rzecz przestrzegania praw podstawowych w Internecie oraz do zabezpieczenia w nadchodzących latach zasadniczych praw i uprawnień.

W naszych postulatach dotyczących DSA skupiamy się na czterech kluczowych obszarach: problematyce odpowiedzialności platform, obowiązkach w zakresie interoperacyjności, sprawiedliwości proceduralnej i większej kontroli w rękach użytkowników. Wprowadzając zasady przyświecające działaniom politycznym, nasze przesłanie dla UE jest jasne: Należy zachować to, co

sprawnie działa. Należy naprawić to, co nie działa lub zostało zepsute. A przede wszystkim należy przywrócić użytkownikom prawo i możliwości kontroli.

Ograniczona odpowiedzialność i brak monitorowania: Należy zachować to, co sprawnie działa

Zasada 1: Pośrednicy online nie powinni ponosić odpowiedzialności za treści użytkowników

Pośrednicy mają do odegrania kluczową rolę w zapewnianiu dostępności treści i rozwoju Internetu. Stanowią czynnik warunkujący wolność słowa, ponieważ umożliwiają ludziom udostępnianie treści odbiorcom na niespotykaną dotąd skalę. Jedną z przyczyn sukcesu pośredników internetowych jest swoisty immunitet, jakim cieszą w odniesieniu do treści osób trzecich.

Jest to jedna z najważniejszych zasad, które naszym zdaniem muszą nadal stanowić podstawę regulacji Internetu: Platformy nie powinny ponosić odpowiedzialności za pomysły, obrazy, filmy lub słowa, które użytkownicy publikują lub udostępniają online. Gdyby taka zasada nie istniała, platformy byłyby zmuszone do monitorowania i zatwierdzenia zachowań użytkowników; filtrowałyby i sprawdzały treści użytkowników; blokowałyby i usuwały wszystko, co kontrowersyjne, budzące zastrzeżenia lub potencjalnie niezgodne z prawem, żeby uniknąć ewentualnej odpowiedzialności prawnej. Z tego samego powodu użytkownicy najprawdopodobniej nie czuliby się chętni ani gotowi do swobodnego wypowiadania się; unikaliby dzielenia się swoją artystyczną ekspresją bądź publikowania krytycznego eseju na temat wydarzeń politycznych. Co gorsza, bez ochrony prawnej usługodawcy mogliby z łatwością stać się celami dla korporacji, rządów lub innych jednostek działających w złej wierze i dążących do wyciszenia użytkowników.

UE powinna zatem dopilnować, żeby pośrednicy internetowi nadal korzystali z kompleksowych wyłączeń i zwolnień z odpowiedzialności oraz nie ponosili odpowiedzialności za treści dostarczane przez użytkowników. Należy zrezygnować przy procedurze ubiegania się o zwolnienia z obecnego mglistego rozróżnienia między pasywnymi i aktywnymi dostawcami usług hostingu: Pośrednicy nie powinni ponosić odpowiedzialności za treści użytkowników, o ile nie są zaangażowani we współtworzenie czy modyfikację tych treści w

sposób, który w znacznym stopniu przyczynia się do niezgodności z prawem i pod warunkiem, że nie posiadają oni faktycznej wiedzy na temat jego niezgodnego z prawem lub naruszającego prawo charakteru. Wszelkie dodatkowe obowiązki muszą być proporcjonalne i nie mogą ograniczać swobody wypowiedzi użytkowników oraz nie mogą być hamulcem dla innowacyjności.

Zasada 2: Tylko orzeczenia sądowe powinny skutkować pociągnięciem do odpowiedzialności

Pośrednicy nie powinni ponosić odpowiedzialności za to, że postanowili nie usuwać treści tylko dlatego, że otrzymali prywatne zawiadomienie od użytkownika. Żeby chronić wolność słowa, UE powinna przyjąć zasadę, zgodnie z którą faktyczną wiedzę o niezgodności z prawem pośrednicy uzyskują dopiero wówczas, gdy otrzymają stosowne orzeczenie sądowe. O zgodności z prawem treści użytkowników powinny decydować niezależne organy sądowe, a nie platformy czy inni niezadowoleni użytkownicy. Wszelkie wyjątki od tej zasady powinny ograniczać się do treści wyraźnie niezgodnych z prawem, czyli treści w sposób oczywisty prawnie niedozwolonych niezależnie od kontekstu. Zawiadomienia o takiej treści powinny być wystarczająco precyzyjne i uzasadnione.

Zasada 3: Zakaz obowiązkowego monitorowania lub filtrowania

Zakaz ogólnego monitorowania na mocy obowiązującej dyrektywy w sprawie handlu elektronicznego ma na celu ochronę użytkowników poprzez zagwarantowanie im wolności wypowiedzi oraz prawa do ich własnych danych osobowych zgodnie z zapisami Karty Praw Podstawowych. Ewentualna rezygnacja z tej ważnej zasady miałaby nie tylko katastrofalne konsekwencje dla wolności użytkowników, ale również nieuchronnie doprowadziłoby do regulacji równoległej, czyli sprywatyzowanego egzekwowania przepisów przez platformy bez przejrzystości, odpowiedzialności ani innych zabezpieczeń.

Państwa członkowskie Unii Europejskiej nie powinny zatem mieć możliwości nakładania na dostawców usług cyfrowych obowiązku monitorowania i zatwierdzenia treści na swoich platformach lub w sieciach pod kątem treści niezgodnych z prawem, które użytkownicy zamieszczają, przesyłają lub przechowują. Platformy nie powinny również mieć ogólnego obowiązku aktywnego monitorowania faktów ani okoliczności wskazujących na niezgodną z prawem działalność użytkowników. Zakaz ogólnego obowiązku w zakresie monitorowania powinien obejmować też zakaz obowiązkowych zautomatyzowanych systemów filtrowania, które oceniają zgodność z prawem treści osób trzecich lub zapobiegają (ponownemu) przesyłaniu niezgodnych z prawem treści. Ponadto żadna odpowiedzialność nie powinna występować w razie niewykrycia przez pośrednika treści niezgodnych z prawem. W tym kontekście należy również chronić powiązane prawa do prywatności takie jak prawo do niepodlegania zautomatyzowanemu systemowi podejmowania indywidualnych decyzji.

Zasada 4: Ograniczenie zakresu nakazów usunięcia treści

Ostatnie przypadki uzmysławiają nam ogólnoświatowe zagrożenia związane z nakazami usuwania treści. W wyroku w sprawie Glawischnig-Piesczek Trybunał Sprawiedliwości UE orzekł, że sąd państwa członkowskiego może nakazać platformom nie tylko usuwanie treści zniesławiających na całym świecie, ale również likwidację innych identycznych lub „równoważnych" materiałów. Orzeczenie rodzi zatrważające skutki, ponieważ przedmiotowa treść może być uznana za niezgodną z prawem w jednym państwie, ale może być absolutnie zgodna z prawem w wielu innych państwach. Odnosząc się również do „zautomatyzowanych technologii" do wykrywania podobnie brzmiących treści, sąd otworzył bramy dla monitorowania za pomocą filtrów, które są notorycznie niedokładne i podatne na nadmierne blokowanie zgodnych z prawem materiałów.

Reforma prawodawstwa UE w zakresie Internetu jest okazją do uznania, że Internet ma charakter globalny, a nakazu usuwania treści o zasięgu globalnym są ogromnie niesprawiedliwe i naruszają wolność użytkowników. Nowe przepisy powinny gwarantować, że orzeczenia sądowe – a w szczególności nakazy i zakazy na zabezpieczenie roszczeń – nie będą stosowane w celu nakładania prawa jednego kraju na każde inne państwo na świecie. Nakazy usuwania treści powinny ograniczać się do przedmiotowej treści i opierać się na zasadach konieczności oraz proporcjonalności pod względem zakresu geograficznego. W przeciwnym razie możliwe jest, że rząd jednego kraju będzie dyktował, co mieszkańcy innych krajów mogą powiedzieć, oglądać lub udostępniać online. Prowadziłoby to do „równi pochyłej" w kierunku budowy coraz bardziej restrykcyjnego globalnego Internetu.

Obowiązki interoperacyjne: Wzmocnienie pozycji użytkowników i innowatorów

Zasada 1: Ogólne obowiązki interoperacyjne

Wizją EFR jest system prawny, który sprzyja innowacjom i przywraca użytkownikom kontrolę nad ich danymi, prywatnością i doświadczeniami online. Uważamy, że interoperacyjność ma do odegrania ważną rolę w urzeczywistnieniu tego rodzaju wizji Internetu o wysokiej użyteczności publicznej, dlatego proponujemy zobowiązania w zakresie interoperacyjności dla platform o znaczącej pozycji rynkowej. Nasze postrzeganie i rozumienie jest proste: platformy, które kontrolują znaczące udziały w rynkach i działają jako strażnicy na takich rynkach, muszą oferować możliwości interoperacyjności z ich kluczowymi funkcjonalnościami dla konkurencyjnych, nowo powstających platform.

Chociaż Europejczycy mają już prawo do przenoszenia danych na podstawie RODO, prawo to wiąże się z szeregiem ograniczeń. Przede wszystkim prawo to nie ma charakteru całościowego (użytkownicy nie mogą przenieść wszystkich danych osobowych), ma charakter warunkowy (możliwe tylko wtedy, gdy jest to „technicznie wykonalne") i nie jest jasne, dokąd użytkownicy powinni przenosić swoje dane. Interoperacyjność jest brakującym elementem, który tchnie życie w prawo przenośności danych. Interoperacyjność poprzez interfejsy techniczne umożliwiłaby użytkownikom komunikowanie się ze znajomymi ponad granicami platformy lub śledzenie ich ulubionych treści na różnych platformach bez konieczności tworzenia kilku kont. Użytkownicy nie byliby już z obawy przed utratą sieci społecznościowej zmuszani do pozostania na platformie, która lekceważy ich prywatność, potajemnie gromadzi ich dane lub zagraża ich bezpieczeństwu. Zamiast tego użytkownicy mieliby możliwość dokonywania faktycznych i świadomych wyborów.

Zasada 2: Delegowalność

Problem jednak na tym się nie kończy. Interoperacyjność powinna również mieć miejsce na poziomie interfejsów użytkownika i powinna zapewniać tyle elastyczności i różnorodności, ile chcą użytkownicy. W związku z platformy o znaczącej pozycji rynkowej powinny umożliwiać również konkurującym z nimi osobom trzecim działanie w imieniu i na zlecenie użytkowników. Jeśli użytkownicy tego chcą, powinni mieć możliwość przekazania elementów swojego doświadczenia online różnym kompetentnym podmiotom. Na przykład, jeśli nie lubisz praktyk moderowania treści na Facebooku, musisz mieć możliwość powierzenia tego zadania innej organizacji, takiej jak organizacja non-profit specjalizująca się w społecznościowym moderowaniu treści.

Zasada 3: Ograniczenie komercyjnego wykorzystania danych

Żeby uniknąć nadużywania interoperacyjności, wszelkie dane udostępniane w ramach interoperacyjności nie powinny być dostępne do ogólnego użytku komercyjnego. Większość głównych platform działa według modeli biznesowych, które opierają się na (często pożądanym) gromadzeniu i sprzedaży danych użytkowników, tym samym dokonując monetyzacji zainteresowania użytkowników i wykorzystując ich dane osobowe. W związku z tym wszelkie dane udostępniane dla celów interoperacyjności powinny być wykorzystywane wyłącznie na potrzeby zapewnienia interoperacyjności, ochrony prywatności użytkowników lub zagwarantowania bezpieczeństwa danych. Zakazując komercyjnego wykorzystania danych mających służyć wdrażaniu lub utrzymywaniu interoperacyjności, chcemy również pozytywnie zachęcić konkurentów do stosowania innowacyjnych, odpowiedzialnych i chroniących prywatność modeli biznesowych.

Zasada 4: Prywatność

Kluczowe znaczenie ma umożliwienie użytkownikom przejęcia kontroli nad tym, w jaki sposób, kiedy, dlaczego i komu udostępniane są ich dane. Oznacza to, że kluczowe zasady leżące u podstaw RODO i innych obowiązujących przepisów, takie jak minimalizacja danych, prywatność już w fazie projektowania i domyślna prywatność muszą być bezwzględnie przestrzegane. Problematyka powinna również obejmować łatwe w użyciu interfejsy, za pośrednictwem których użytkownicy mogą udzielić wyraźnej zgody na jakiekolwiek wykorzystanie swoich danych (a także mogą w każdej chwili cofnąć wcześniej udzieloną zgodę).

Zasada 5: Bezpieczeństwo

Dane i komunikacja użytkowników powinny być jednocześnie nie tylko poufne, ale również bezpieczne. Środki na rzecz interoperacyjności powinny zawsze koncentrować się na bezpieczeństwie użytkowników i nigdy nie powinny być traktowane jako powód uniemożliwiający platformom podejmowanie wysiłków w celu zapewnienia użytkownikom właściwego poziomu bezpieczeństwa. Jeżeli jednak pośrednicy muszą zawiesić interoperacyjność w celu rozwiązania problemów związanych z bezpieczeństwem, nie powinni wykorzystywać takich sytuacji do zerwania zasad interoperacyjności w ogóle, lecz raczej winni komunikować się w sposób przejrzysty, rozwiązać problem i przywrócić interfejsy interoperacyjności w uzasadnionych oraz jasno określonych ramach czasowych.

Zasada 6: Dokumentacja i brak dyskryminacji

Wreszcie kluczowe znaczenie ma dopilnowanie, żeby interoperacyjność nie stała się narzędziem dla potężnych zasiedziałych operatorów do pełnienia funkcji strażników i dalszego umacniania ich dominującej

pozycji. Formułowanemu przez nas postulatowi wzmocnienia pozycji użytkowników najlepiej służy sytuacja jak największej różnorodności i pluralizmu, czyli interoperacyjność powinna przynosić korzyści jak największej liczbie konkurentów, a nie tylko kilku preferowanym podmiotom. Żeby zapewnić użytkownikom większy wybór, dostęp do interfejsów interoperacyjności nie powinien dyskryminować różnych konkurentów i nie powinien wiązać się z surowymi zobowiązaniami ani ograniczeniami zakresu treści. Interfejsy interoperacyjności, takie jak interfejsy API, muszą być łatwo dostępne, dobrze udokumentowane oraz jasne i przejrzyste.

Należy stawiać użytkowników na pierwszym miejscu: Zaoferowanie użytkownikom możliwości i środków rygorystycznej kontroli

Zasada 1: Dajmy użytkownikom kontrolę nad treścią

Wiele serwisów, takich jak Facebook i Twitter, pierwotnie prezentowało ściśle chronologiczną listę postów znajomych użytkowników. Z biegiem czasu większość dużych platform zamieniła prezentację chronologiczną na bardziej złożone (i nieprzejrzyste) algorytmy porządkujące, regulujące i rozpowszechniające treści, w tym reklamy i inne promowane materiały. Algorytmy, rozwijane i opracowywane przez platformę, niekoniecznie koncentrują się na zaspokajaniu potrzeb użytkowników, ale zazwyczaj dążą wyłącznie do maksymalizacji czasu i uwagi odbiorców na danej stronie internetowej. Posty z większym „zaangażowaniem" są traktowane priorytetowo, nawet jeśli zaangażowanie to jest napędzane silnymi emocjami, takimi jak gniew lub rozpacz sprowokowana przez post. Podczas gdy użytkownicy czasami mogą wrócić do strumienia chronologicznego, struktura i projekt interfejsów platform często zniechęcają ich do tego lub nakłaniają do przejścia z powrotem do sugerowanego układu. Interfejsy wprowadzające w błąd lub manipulujące użytkownikami, w tym praktyki „dark pattern", są często sprzeczne z podstawowymi zasadami europejskich przepisów o ochronie danych, a uregulowania w ich przedmiocie powinny zostać stosownie uwzględnione w ustawie o usługach cyfrowych.

Narzędzia algorytmiczne platform wykorzystują prywatną wiedzę o użytkownikach, zebraną z tysięcy pozornie niezwiązanych ze sobą punktów danych. Wiele wniosków wyciągniętych z tych danych jest zupełnie nieoczekiwanych dla użytkowników: platformy mają dostęp do danych, które sięgają dalej niż większość użytkowników wydaje się zdawać sobie sprawę i są w stanie wyciągać wnioski zarówno z indywidualnych, jak i zbiorowych zachowań. Założenia dotyczące preferencji użytkowników są zatem często formułowane poprzez wnioskowanie z pozornie niezwiązanych ze sobą punktów danych. Może to kształtować (i często ograniczać) sposoby, w jakie użytkownicy mogą wchodzić w interakcje z treściami online, a także wzmacniać błędne informacje i polaryzację w sposób, który może podważać przejrzystą, świadomą wymianę informacji, na których zbudowane są społeczeństwa demokratyczne.

Użytkownicy nie muszą akceptować takiego stanu rzeczy. Istnieje wiele wtyczek zewnętrznych firm, które zmieniają wygląd i zawartość platform społecznościowych zgodnie z indywidualnymi potrzebami i preferencjami. Teraz jednak większość z tych wtyczek wymaga wiedzy technicznej, żeby je odkryć i zainstalować, a platformy mają silną motywację do ukrywania i zapobiegania popularyzacji takich niezależnych narzędzi wśród użytkowników. DSA jest doskonałą okazją dla Europy do stworzenia bardziej przyjaznego otoczenia prawnego, żeby zachęcać i wspierać ten zorientowany na użytkownika rynek. Regulacja powinna sprzyjać interoperacyjności i umożliwiać zgodność z zasadami konkurencji. Powinna też ustanawiać wyraźne, egzekwowalne przepisy na rzecz przeciwdziałania nadmiernie agresywnym warunkom świadczenia usług, które mają na celu zakazywanie wszelkiego przekonstruowania oraz inżynierii odwrotnej i wzajemnych połączeń. Poza ustawą o usługach cyfrowych UE musi aktywnie wspierać w Europie projekty open source i projekty komercyjne, które oferują platformom zlokalizowane rozwiązania front-end lub rozwiązania front-end wzmacniające pozycję użytkowników, a także wspierać dynamiczny i rentowny rynek tych narzędzi.

Zapewnienie jednostkom – w przeciwieństwie do platform – większej kontroli nad treścią jest kluczowym krokiem w celu rozwiązania niektórych z najbardziej powszechnych problemów świata online, którymi obecnie zarządza się nieskutecznie lub niewłaściwie poprzez praktyki moderowania treści. Środki kontroli dostępne dla użytkowników nie powinny wymagać podwyższonego poziomu znajomości technologii niezbędnego do bezpiecznego poruszania się w sieci.
Zamiast tego użytkownicy platform mediów społecznościowych o znaczącej pozycji rynkowej powinni w prosty i przyjazny dla użytkownika sposób mieć możliwość wyboru treści, z którymi chcą wchodzić w interakcje, a także rezygnacji z treści, których nie chcą widzieć. Użytkownicy powinni mieć również możliwość całkowitego odrzucenia rekomendacji polecanych algorytmicznie bądź wyboru innej heurystyki porządkowania treści.

Zasada 2: Przejrzystość algorytmiczna

Oprócz większej kontroli nad treściami, z którymi wchodzą w interakcje, użytkownicy zasługują też na większą przejrzystość ze strony firm, żeby w pełni zrozumieć, dlaczego treści lub wyniki wyszukiwania są im pokazywane albo są przed nimi ukrywane. Platformy internetowe powinny dostarczać istotnych informacji na temat narzędzi algorytmicznych, których używają przy moderacji treści (tj. systemów rekomendacji treści, narzędzi do oznaczania treści) i dopasowywania treści (na przykład przy tworzeniu rankingu lub obniżeniu pozycji treści w rankingu). Platformy powinny również oferować łatwo dostępne wyjaśnienia, które pozwolą użytkownikom zrozumieć, kiedy, do jakich zadań i w jakim zakresie wykorzystywane są narzędzia algorytmiczne. Żeby zmniejszyć skalę wysiłków i nakładów potrzebnych ze strony indywidualnych użytkowników dla zrozumienia, w jaki sposób wykorzystywane są algorytmy, platformy o znaczącej pozycji rynkowej powinny umożliwiać niezależnym naukowcom i odpowiednim organom regulacyjnym audyt swoich narzędzi algorytmicznych w celu upewnienia się, że są one wykorzystywane zgodnie z przeznaczeniem.

Zasada 3: Odpowiedzialne zarządzanie

Platformy internetowe rządzą swoimi użytkownikami na podstawie ich własnych warunków świadczenia usług, społecznościowych wytycznych lub norm Dokumenty te często wiążą się z podstawowymi zasadami, które określają, co użytkownicy mogą robić na platformie i jakie zachowania są ograniczone. Platformy regularnie aktualizują te dokumenty, często w mniejszym stopniu, ale czasami w znacznym stopniu, a robią to zazwyczaj bez konsultacji ze swoimi użytkownikami bądź bez powiadamiania ich o zmianach. Użytkownicy takich platform muszą być powiadamiani o każdej zmianie zasad, którym podlegają, muszą być każdorazowo proszeni o zgodę na zmianę i powinni być informowani o konsekwencjach dokonywanego w tym zakresie wyboru. Powinni również otrzymywać sensowne wyjaśnienia wszelkich istotnych

zmian w języku, który rozumieją. Co więcej, platformy powinny przedstawiać swoje warunki świadczenia usług w formacie nadającym się do odczytu maszynowego i ułatwiać publiczny dostęp do wszystkich poprzednich wersji swoich warunków świadczenia usług.

Zasada 4: Prawo do anonimowości online

Istnieje niezliczona liczba powodów, dla których jednostki fizyczne mogą nie chcieć publicznie udostępniać swojej tożsamości online. Chociaż anonimowość była kiedyś powszechna w Internecie, coraz trudniej jest ją utrzymać. Decydenci polityczni w UE i poza nią w nadziei na rozwiązanie problemu mowy nienawiści lub „fake newsów" proponują zobowiązanie platform do wymagania pełnego imienia i nazwiska.

Dla wielu osób, jednak, w tym członków społeczności LGBTQ+, pracowników seksualnych i ofiar przemocy domowej, takie zasady mogą mieć druzgocące skutki i prowadzić do nękania lub innych działań o charakterze odwetowym. Zasadniczo uważamy, że państwa członkowskie powinny szanować wolę nieujawniania swojej tożsamości w Internecie przez jednostki. Ustawa o usługach cyfrowych powinna również w tym zakresie potwierdzać samostanowienie informacyjne użytkowników i wprowadzać europejskie prawo do anonimowości w Internecie. Wszelkie rozbieżne warunki świadczenia usług powinny podlegać kontroli uczciwości i rzetelności.

Przejrzystość i sprawiedliwość proceduralna: Należy naprawić to, co nie działa lub zostało zepsute

Zasada 1: Mechanizmy zgłaszania

Pośrednicy nie powinni ponosić odpowiedzialności za to, że postanowili nie usuwać treści tylko dlatego, że otrzymali prywatne zawiadomienie od użytkownika. Z zastrzeżeniem pewnych wyjątków, UE powinna przyjąć zasadę, zgodnie z którą faktyczną wiedzę o niezgodności z prawem pośrednicy uzyskują dopiero wówczas, gdy otrzymają stosowne orzeczenie sądowe.

UE powinna natomiast przyjąć zharmonizowane przepisy dotyczące mechanizmów zgłaszania, które pomogą użytkownikom powiadamiać platformy o potencjalnie niezgodnych z prawem treściach i zachowaniach. Zgłaszanie potencjalnie niezgodnych z prawem treści online brzmi prosto, ale w praktyce może być dość zniechęcające.
Różne platformy wykorzystują różne systemy zgłaszania treści lub działań, a kategorie stosowane do rozróżniania poszczególnych rodzajów treści mogą nie tylko się znacznie różnić, ale mogą być wręcz również mylące i trudne do zrozumienia. Niektóre platformy w ogóle nie oferują sensownych opcji powiadamiania. Zgłaszanie potencjalnie niezgodnych z prawem treści powinno być łatwe, a wszelkie działania następcze podejmowane przez platformę powinny być przejrzyste dla użytkowników.

Zasada 2: Standard przejrzystości i sprawiedliwości w zawiadamianiu i działaniu

Moderowanie treści jest często nieprzejrzyste – firmy zazwyczaj nie udzielają użytkownikom wystarczających informacji na temat tego, jakie wypowiedzi są dopuszczalne lub dlaczego niektóre treści zostały usunięte. Żeby uczynić moderację treści bardziej przejrzystą, platformy powinny powiadamiać użytkowników o usunięciu treści (lub zawieszeniu ich konta). Zawiadomienie powinno wskazywać usuniętą treść, konkretną zasadę, która została uznana za naruszoną, a także sposób wykrycia powyższych treści. Zawiadomienie powinno również zawierać łatwo dostępne wyjaśnienie całego procesu, w ramach którego użytkownik może odwołać się od decyzji.

Platformy powinny zapewniać przyjazny dla użytkownika, widoczny i szybki proces odwoławczy, żeby umożliwić skuteczne rozstrzyganie sporów dotyczących moderowania treści. Mechanizmy odwoławcze muszą być również dostępne, łatwe w użyciu i zgodne z jasno określonym harmonogramem. Powinny umożliwiać użytkownikom przedstawienie dodatkowych informacji i obejmować weryfikację przez człowieka. Po zakończeniu procedury odwoławczej użytkownicy powinni być powiadamiani i otrzymywać oświadczenie wyjaśniające uzasadnienie podjętej decyzji w języku zrozumiałym dla użytkownika. Ważne jest również, żeby użytkownicy byli informowani, że nawet jeśli zdecydują się wziąć udział w procesie rozstrzygania sporów, nie tracą możliwości dochodzenia swoich praw przed niezależnymi organami sądowymi takimi jak sąd ich właściwej jurysdykcji krajowej.

Zasada 3: Otwarcie czarnej skrzynki odpowiedzialnej za automatyczne podejmowanie decyzji

Większość głównych platform wykorzystuje algorytmy do zautomatyzowania części realizowanych przez nie praktyk moderowania treści. Moderowanie treści jest niepewnym i ryzykownym zadaniem i wielu ma nadzieję, że zautomatyzowane narzędzia moderowania treści mogą być srebrną kulą, która rozwiąże szereg problemów w tym zakresie. Niestety moderacja treści jest niechlujna, bardzo zależna od kontekstu i niezwykle trudna do późniejszego naprawienia, a zautomatyzowane narzędzia moderacji popełniają wiele, wiele błędów. Problemy te stały się szczególnie widoczne podczas pandemii COVID-19, ponieważ wiele platform zastąpiło moderatorów ludzkich zautomatyzowanymi narzędziami moderowania treści.

W świetle podstawowych wad zautomatyzowanej moderacji treści platformy powinny zapewniać jak największą przejrzystość korzystania z narzędzi algorytmicznych. Jeżeli platformy wykorzystują zautomatyzowane systemy podejmowania decyzji w celu ograniczenia treści, powinny wskazać, na którym etapie procesu zastosowano narzędzia algorytmiczne, wyjaśnić logikę podejmowania zautomatyzowanych decyzji, a także wyjaśnić, w jaki sposób użytkownicy mogą odwołać się od podjętej decyzji.

Zasada 4: Przywrócenie niewłaściwie usuniętych treści

Zarówno ludzkie, jak i automatyczne systemy moderowania treści wciąż popełniają błędy, które mogą powodować prawdziwe i wymierne szkody. Wysiłki mające na celu moderowanie treści uważanych za obraźliwe lub niezgodne z prawem regularnie wywierają nieproporcjonalny wpływ na grupy już marginalizowane. Moderowanie treści często koliduje z wypowiedziami przeciwko mowie nienawiści, próbami przywrócenia pierwotnego i właściwego sensu określonym terminom lub wywołuje rasizm poprzez dzielenie się wypowiedziami rasistowskimi.

Ponieważ błędne decyzje dotyczące moderowania treści są tak powszechne i mają tak negatywne skutki, istotne jest, żeby platformy przywracały treść użytkowników, gdy decyzji o usunięciu nie można uzasadnić właściwą interpretacją zasad platform lub gdy usunięcie okaże się po prostu błędem. Ustawa o usługach cyfrowych powinna promować szybkie i łatwe przywracanie niesłusznie usuniętych treści lub niesłusznie wyłączonych kont.

Zasada 5: Skoordynowany i skuteczny nadzór regulacyjny

Dobre prawa są kluczowe, ale ich egzekwowanie jest co najmniej tak samo ważne. W związku z tym prawodawcy europejscy powinni zadbać o to, by niezależne organy mogły pociągać platformy do odpowiedzialności. Należy wzmocnić koordynację między niezależnymi organami krajowymi, żeby umożliwić egzekwowanie przepisów w całej UE, a platformy powinny być zachęcane do

przestrzegania obowiązków należytej staranności, na przykład poprzez wymierne sankcje zharmonizowane na poziomie całej Unii Europejskiej.