

Britten moeten identiteit prijsgeven voor online platforms

6 augustus 2025



De Britten moeten hun identiteit/leeftijd bekendmaken als zij gebruik willen maken van de grotere social mediaplatforms. Het heeft geleid tot veel protest maar ook tot een record aan downloads van VPN-software. Wat houdt de Online Safety Bill in, kan VPN helpen en waarom maakt deze wet een einde aan vrij en anoniem internet in het Verenigd Koninkrijk?

Afbeelding: [Pixabay](#)

Groot aantal websites niet meer vrij toegankelijk

Met de introductie van de [Online Safety Act](#) maakt het Verenigd Koninkrijk een einde aan vrij en onbeperkt toegang tot internet. Met deze wet wil de Britse overheid volwassenen “*maar vooral kinderen*” beschermen tegen schadelijke content. Volgens de toelichting op de wet krijgen ouders meer mogelijkheden om te bepalen wat hun kinderen online te zien krijgen.

Een simpel aanvinken van ‘ik ben 18 jaar of ouder’ volstaat niet meer. De wet schrijft voor hoe de leeftijd kan worden vastgesteld. Dat kan onder meer doordat een persoon informatie van zijn bank indient die zijn leeftijd bewijst. Of een foto-ID matching met behulp van gezichtsherkenning. Ook kan een creditcard bewijzen dat iemand 18 jaar of ouder is, immers alleen volwassen Britten kunnen er een krijgen.

Maar de overheid heeft ook geen moeite om het persoonlijke e-mailverkeer door te laten snuffelen of er mailverkeer tussen zit dat wijst op een “*volwassen situatie*”, zoals mailverkeer over het aanvragen van een hypotheek. Vanzelfsprekend mag ook een digitale ID-Portemonnee worden gebruikt. Volgens de toelichting op de wet “*werkt de EU hieraan*”. Ter herinnering, de Britten zijn geen lid meer van de EU, maar wachten ogenschijnlijk wel op digitale-ID van de EU.

De regeling lijkt soepel te zijn omdat ook aan de hand van een selfie door de webbeheerder de leeftijd mag worden ingeschat. Hoe dat gaat met sociale mediaplatforms is onduidelijk. Mark Zuckerberg zal toch niet bereid zijn de pasfoto's te gaan beoordelen.

Een vreemde andere vorm van identificatie houdt in dat de persoon zijn/haar leeftijd moet bewijzen aan zijn/haar mobiele operator die dan vervolgens namens de site de goedkeuring verstrekt. Hoe dat in zijn werk gaat, is onduidelijk.

Welke vorm je ook kiest, je moet je identiteit in enigerlei vorm prijsgeven, om “*kinderen te beschermen*”. Het zal duidelijk zijn dat de identiteit dan ook direct gekoppeld kan worden aan het webbezoek. Dat hiervan al een preventieve werking uitgaat in de vorm van zelfcensuur, moge duidelijk zijn.

Grote user-to-user diensten, bekend als Categorie 1 diensten, zullen volwassen

gebruikers tools aanbieden die, als ze ervoor kiezen om die te gebruiken, hen meer controle geven over het soort inhoud dat ze zien en met wie ze online omgaan. Zo stelt de wet.

User-to-user diensten zijn websites waarbij door uploaden van materiaal contact met anderen tot stand kan worden gebracht. We moeten hier, zonder dat het in de tekst staat, vermoedelijk denken aan X, Facebook of TikTok. Met zo'n 'tool' moet de kans verkleind worden dat je inhoud ziet van een 'niet-geverifieerde gebruiker'. Daarmee blijkt daarmee ook de volwassene doel van deze act. X maakt al onderscheid tussen beide categorieën. Vooralsnog kan content van een niet-geverifieerde gebruiker een geverifieerde gebruiker bereiken, maar de vraag is hoe lang nog.

Bescherming tegen mis- of disinformatie

Met deze wet grijpt de overheid ook in op de online gedeelde inhoud. Online media moeten letten op *“door staten verspreide mis- en disinformatie”*. Het gaat om buitenlandse 'state actors'. De eigen overheid mag klaarblijkelijk gewoon haar eigen mis- en disinformatie verspreiden. Een adviescommissie van '[Ofcom](#)', een nieuw toezichthoudend orgaan, zal bepalen wat onder mis- en disinformatie moet worden verstaan.

Vooraf bezoekers van pornografische websites zullen met een leeftijdcheck worden geconfronteerd. De voornoemde Ofcom heeft onderzoek ingesteld naar 34 van dergelijke websites of zij wel een leeftijdscheck doen. Met 9 miljoen maandelijkse Britse bezoekers heeft deze categorie *“ter bescherming van kinderen”* de hoogste prioriteit.

Ofcom kan boetes opleggen tot £18 miljoen of 10% van de in aanmerking komende wereldwijde inkomsten, afhankelijk van welke groter is.

“In ernstige gevallen, kunnen we een gerechtelijk bevel vragen voor ‘business disruption measures’, zoals het eisen van betalingsproviders of adverteerders om hun diensten van een platform in te trekken, of het eisen van internetproviders om de toegang tot een site in het Verenigd Koninkrijk te blokkeren.”

VPN om de check te omzeilen

Aanbieders van VPN-diensten zagen direct na het ingaan van de wet op 25 juli jl. de installatie van hun software in het VK verveelvoudigen. De als goed bekendstaande Zwitserse aanbieder Proton zag een toename van 1.400% van gedownloade VPN-software.

Met VPN, Virtual Private Network, kan het eigen IP-adres, gekoppeld aan de eigen internet service provider, worden vervangen door een die niet aan de eigen internet service provider (ISP) is gekoppeld. Deze techniek wordt al veel gebruikt in landen met een strenge censuur, waaronder nu dus ook de Britse eilanden vallen.

Toch kan ook het gebruik van VPN-diensten worden verboden zoals onder andere in Rusland, China en Noord-Korea. ([Meer landen](#)). Naast een verbod worden de diensten ook technisch geblokkeerd. China heeft voor controle op het (illegale) gebruik de meest vergaande techniek: deep packet inspection (DPI). Buitenlandse bedrijven mogen in China wel van VPN gebruik maken.

Ook Rusland is geen kampioen vrijheid van meningsuiting. Na protesten in 2012 heeft Rusland een lijst van verboden websites opgesteld. De lijst was in eerste instantie gericht op kinderpornosites, maar groeide snel uit tot dubbelzinnige categorieën zoals 'schending van de gevestigde orde' en 'oproepen tot illegale bijeenkomsten'. In November 2017 verbood Rusland VPN-diensten, Tor en proxies, allemaal tools die mensen kunnen gebruiken om toezicht te vermijden. De Russische overheid was bijzonder streng met VPN-diensten die weigerden gebruikersgegevens in te dienen voor inspectie door de overheid. Ondanks deze maatregelen wordt nog steeds gebruik gemaakt van VPN, maar dat is niet zonder risico.

Het is mogelijk om te zien wanneer een internetgebruiker VPN gebruikt. Een internet service provider (ISP) kan zien dat er een ander IP-adres wordt gebruikt dan gebruikelijk, al kan men niet zien welke websites hiermee worden bezocht. De meeste IP-adressen die VPN-diensten gebruiken zijn bekend en kunnen dus actief worden gezien en geblokt.

In een van komende nieuwsbrieven van EZAZ zullen wij meer tips geven over het gebruik van VPN.

De Britse overheid is vooralsnog niet van plan om het gebruik van VPN aan banden te leggen, maar zegt “*de ontwikkelingen nauwgezet te monitoren*”. Ondanks strenge maatregelen kunnen gebruikers in beperkende landen stappen ondernemen om VPN-blokkades te omzeilen. Daar zijn ook weer speciale tools voor.

De Britse toezichthouder Ofcom [vertelde de BBC](#) dat het volgens de Online Safety Act illegaal zal zijn voor platforms om het gebruik van VPN aan te moedigen: Ouders moeten er zich van bewust zijn dat kinderen die een VPN gebruiken om toegang te krijgen tot internet “*niet kunnen **profiteren van de bescherming van de Online Safety Act***”.

(Accentuering, red.)

[Uitgebreide informatie over de Online Safety Act](#)