DOC 56 **1039/001**

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

12 september 2025

VOORSTEL VAN RESOLUTIE

betreffende de opheffing van online anonimiteit en de instelling van een doeltreffende leeftijdscontrole voor toegang tot sociale media

(ingediend door de heer Ismaël Nuino)

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

12 septembre 2025

PROPOSITION DE RÉSOLUTION

visant à mettre fin à l'anonymat en ligne et à instaurer un contrôle effectif de l'âge pour l'accès aux réseaux sociaux

(déposée par M. Ismaël Nuino)

N-VA	:	*Nieuw-Vlaamse Alliantie*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
PS	:	*Parti Socialiste*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Les Engagés	:	*Les Engagés*
Vooruit	:	*Vooruit*
cd&v	:	*Christen-Democratisch en Vlaams*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
Open Vld	:	*Open Vlaamse liberalen en democraten*
DéFI	:	*Démocrate Fédéraliste Indépendant*
ONAFH/INDÉP	:	*Onafhankelijk-Indépendant*

Afkorting bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 56 0000/000	*Parlementair document van de 56e zittingsperiode + basisnummer en volgnummer*	*DOC 56 0000/000*	*Document de la 56e législature, suivi du numéro de base et numéro de suivi*
QRVA	*Schriftelijke Vragen en Antwoorden*	*QRVA*	*Questions et Réponses écrites*
CRIV	*Voorlopige versie van het Integraal Verslag*	*CRIV*	*Version provisoire du Compte Rendu Intégral*
CRABV	*Beknopt Verslag*	*CRABV*	*Compte Rendu Analytique*
CRIV	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*	*CRIV*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN	*Plenum*	*PLEN*	*Séance plénière*
COM	*Commissievergadering*	*COM*	*Réunion de commission*
MOT	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT*	*Motions déposées en conclusion d'interpellations (papier beige)*

TOELICHTING

DAMES EN HEREN,

1. ***Online anonimiteit: de blinde vlek van de rechtsstaat***

De 21e eeuw wordt gekenmerkt door het belang van de digitale ruimte. Dat inmiddels evidente gegeven is echter nog niet volledig doorgedrongen in de manier waarop de collectieve normen en individuele verantwoordelijkheden gestalte krijgen. In een rechtsstaat is elke burger vrij om te handelen, zich uit te spreken, kritiek te uiten en te creëren, maar die vrijheid is onlosmakelijk verbonden met de vereiste om verantwoording af te leggen voor zijn daden. De legitimiteit van de gemeenschappelijke regels berust op die wisselwerking, die dienstdoet als een pact dat een politieke invulling geeft aan het concept "vrijheid". Vandaag is die samenhang tussen vrijheid en verantwoordelijkheid echter grotendeels verdwenen in de digitale ruimte. In dat opzicht is de algemene anonimiteit op de digitale platformen een van de meest zorgwekkende blinde vlekken, want ze zet onze hedendaagse opvatting van het begrip "rechtsstaat" op de helling.

Door de anonimiteit op het internet kan eender wie in de openbare ruimte zijn gang gaan (commenten, posten, influencen of dreigen) zonder dat zijn echte identiteit wordt gecheckt of zelfs maar kan worden achterhaald, tenzij via een ingewikkelde juridische procedure. Het gaat hier niet om een randfenomeen, maar om een zeer groot deel van de online interacties, met name op sociale media, fora en berichten- of streamingapps. Die massale anonimiteit doet meer dan gewoon borg staan voor discretie of democratische ademruimte, maar heeft daarentegen de kwaliteit van het publieke debat ingrijpend veranderd, het vertrouwen tussen burgers aangetast en het vermogen van de staat om de wet te handhaven verzwakt.

Wat in het echte leven verboden is (beledigen, belagen, bedreigen, racistische of seksistische haat zaaien, de publieke opinie kwaadwillig manipuleren) kan op het internet vandaag vrijwel gegarandeerd straffeloos. Dat is niet het gevolg van een rechtsvacuüm; de teksten bestaan, zoals de in het Strafwetboek opgenomen misdrijven, de antidiscriminatiewetgeving, bepalingen met betrekking tot privacy of laster. Een onwettig betoog is echter vaak zeer moeilijk of zelfs onmogelijk met de persoon erachter in verband te brengen omdat digitale platformen de identiteit van de accounthouder niet controleren. Door tijdelijke e-mailadressen, nepprofielen, VPN's en meerdere nicknames wordt het extreem moeilijk of zelfs onmogelijk die personen te bestraffen of zelfs

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

1. ***L'anonymat en ligne, l'angle mort de l'État de droit***

Le XXIe siècle est caractérisé par l'importance de l'espace numérique. Ce constat, s'il est désormais une évidence, n'est pas encore pleinement intégré dans notre manière de concevoir les normes collectives et les responsabilités individuelles. Dans toute société régie par l'État de droit, chaque citoyen est libre d'agir, de s'exprimer, de critiquer, de créer mais cette liberté est indissociable d'une exigence, celle répondre de ses actes. C'est ce lien qui fonde la légitimité des règles communes, c'est ce pacte qui donne à la liberté son contenu politique. Or, dans l'espace numérique, ce lien entre liberté et responsabilité est aujourd'hui largement rompu. L'anonymat généralisé sur les plateformes numériques constitue, à ce titre, l'un des angles morts les plus préoccupants, allant à l'encontre de notre conception contemporaine de l'État de droit.

L'anonymat en ligne permet à quiconque d'intervenir dans l'espace public (qu'il s'agisse de commenter, de publier, d'influencer ou de menacer) sans que son identité réelle soit vérifiée, ni même vérifiable sans une procédure judiciaire complexe. Ce phénomène n'est pas marginal; il concerne une part très importante des interactions numériques, en particulier sur les réseaux sociaux, les forums, les applications de messagerie ou de vidéo en direct. Loin de garantir une simple discrétion ou un espace de respiration démocratique, cet anonymat de masse a, dans la pratique, profondément altéré la qualité du débat public, érodé la confiance entre les citoyens et affaibli la capacité de l'État à faire respecter le droit.

Ce qui est interdit dans la vie réelle (proférer des injures, harceler une personne, menacer, diffuser de la haine raciale ou sexiste, manipuler l'opinion publique à des fins malveillantes) peut aujourd'hui se faire en ligne avec une impunité quasi garantie. Cette réalité ne résulte pas d'un vide juridique; les textes existent, comme les infractions qui sont prévues par le Code pénal, la législation anti-discrimination, les dispositions relatives à la vie privée ou à la calomnie. Mais le lien entre le propos illégal et l'auteur est souvent trop difficile, voire impossible, à établir car les plateformes numériques ne vérifient pas l'identité de ceux qui y créent des comptes. Les adresses e-mail temporaires, les faux profils, les VPN, les pseudonymes multiples rendent extrêmement

maar te verhoren. Daardoor verliest de wet haar grip en verwordt ze tot een vodje papier.

Die discrepantie leidt tot ontwrichting, tot een soort democratische dissonantie: aan de ene kant zijn er de instellingen die principes voorstaan (tolerantie, gelijkheid, waardigheid, haatbestrijding) en aan de andere kant is er een ruimte waar die principes dagelijks met voeten worden getreden zonder gepaste reactie. Dat is geen technisch, maar een groot politiek probleem: het gaat om de daadwerkelijke uitoefening van het recht in een omgeving die ons collectieve leven vormgeeft. De rechtsstaat mag niet stoppen waar de digitale wereld begint.

Digitale platformen zijn de belangrijkste fora voor het publieke debat geworden en nemen *de facto* een steeds groter deel van de regulerende functie over die normaal de soevereine staat zou moeten uitoefenen. Op de digitale platformen wordt beslist wat aanvaardbaar is, wat wordt gerapporteerd, wat verborgen blijft of wordt gepromoot. Dat gebeurt echter niet op basis van een democratisch mandaat of in naam van het algemeen belang, maar uit commerciële, technologische of opportunistische overwegingen. Anonimiteit wordt in die context een hefboom om alles los te laten: sociale remmingen worden overboord gegooid, meningsverschillen op de spits gedreven en standpunten verkondigd zonder enige vorm van fatsoen maar voortgestuwd door een systeem dat de drang om te scoren voedt. Platformen hebben geen structureel belang bij minder anonimiteit; anonimiteit is een hoeksteen van hun bedrijfsmodel.

De democratische staten hebben lang geaarzeld om iets tegen die gang van zaken te ondernemen. Ze vreesden dat elke aantasting van de anonimiteit zou worden beschouwd als een aanval op de vrijheid van meningsuiting en zelfs op de persoonlijke levenssfeer. Ze hebben de voorkeur gegeven aan zelfregulering door de platformen, gevolgd door flankerende maatregelen via verordeningen als de *Digital Services Act* (DSA); hoe belangrijk ook, ze gaat voorbij aan de anonimisering. Nochtans zijn de waarschuwingen legio, constant en gelijklopend. Het ene na het andere rapport documenteert de omvang van online geweld, de schade door cyberpesten, de weerslag op de geestelijke gezondheid, de enorme toename van desinformatiecampagnes, de focus op kwetsbare groepen enzovoort.

Het is niet de bedoeling anonimiteit als zodanig in de ban te slaan. In sommige gevallen blijft die noodzakelijk, bijvoorbeeld voor klokkenluiders, activisten in autoritaire regimes of slachtoffers van geweld die willen getuigen. In het dagelijkse gebruik van sociale media in onze democratieën is anonimiteit echter synoniem geworden voor straffeloosheid. Ze beschermt niet de zwakken, maar de

difficile, voire impossible, toute tentative de sanction ou même de simple interpellation. Dans cette configuration, la loi n'a plus de prise, elle devient seulement théorique.

Ce décalage crée un désordre profond. Il introduit une forme de dissonance démocratique; d'un côté, des institutions qui proclament des principes (tolérance, égalité, dignité, lutte contre la haine) et, de l'autre, un espace où ces principes sont quotidiennement piétinés sans réaction proportionnée. Il ne s'agit pas ici d'un problème technique mais bien d'un problème politique majeur; celui de l'effectivité du droit dans un environnement structurant de notre vie collective. L'État de droit ne peut pas s'arrêter aux portes du numérique.

Les plateformes numériques, devenues les principales médiatrices de la parole publique, ont, de fait, hérité d'une part croissante de la fonction régulatrice qui devrait normalement être exercée par l'État souverain. Elles décident de ce qui est acceptable, de ce qui est signalé, de ce qui est masqué ou promu; mais elles ne le font pas sur la base d'un mandat démocratique ni au nom d'un intérêt général; elles le font selon des logiques commerciales, technologiques ou opportunistes. L'anonymat, dans ce système, est un levier libérant toutes sortes de pulsions; il libère les expressions sociales des inhibitions, il suscite la polémique, il alimente des formes de participation sans aucune forme de civilité mais profitant aux indicateurs de performance. Les plateformes n'ont, structurellement, aucun intérêt à réduire l'anonymat; il est un ingrédient actif de leur modèle économique.

Face à cette situation, les États démocratiques ont longtemps hésité. Ils ont redouté que toute remise en question de l'anonymat soit perçue comme une atteinte à la liberté d'expression, voire à la vie privée. Ils ont privilégié l'autorégulation des plateformes, puis l'encadrement par des règlements comme le *Digital Services Act* (DSA), qui, bien qu'important, ne traite pas de la question de l'anonymat. Pourtant, les alertes sont multiples, constantes, convergentes. Les rapports se succèdent pour documenter l'ampleur des violences en ligne, les ravages du cyberharcèlement, l'impact sur la santé mentale, la prolifération des campagnes de désinformation, le ciblage de groupes vulnérables.

Il ne s'agit pas ici de jeter l'anathème sur l'anonymat en tant que tel. Dans certains cas, il reste un outil nécessaire, comme par exemple pour les lanceurs d'alerte, les militants dans des régimes autoritaires, les victimes de violences qui souhaitent témoigner. Mais, dans l'usage courant des réseaux sociaux dans nos démocraties, l'anonymat absolu est devenu synonyme d'impunité. Il

daders. Ze bevordert het debat niet, maar verstoort het. Ze garandeert de vrijheid van meningsuiting niet, maar holt de betekenis en de draagwijdte ervan uit.

Een volwassen democratie mag niet tolereren dat de digitale publieke ruimte aan elke vorm van verantwoordelijkheid ontsnapt. Ze mag niet dulden dat de slachtoffers moeten kiezen tussen zwijgen of het publiekelijk tentoonspreiden van hun leed, zonder effectief in het verweer te kunnen treden tegen hun aanvallers. Ze mag niet, op haar eigen grondgebied, de gevolgen blijven ondergaan van een elders ontworpen interactiemodel zonder transparantie, zonder rechtvaardigheid, zonder duidelijke regels.

De tijd is dan ook rijp voor een grootschalige beleidsingreep: de digitale actoren moeten individueel voor hun verantwoordelijkheid worden gesteld, zulks niet op basis van veralgemeend toezicht of afschaffing van de privacy, maar van de concrete, bij wet gewaarborgde mogelijkheid de dader van online misbruik te kunnen identificeren wanneer de wet dat vereist. Zulks betekent niet dat iedereen zijn naam moet bekendmaken; het is zaak een systeem op te zetten waarin elke digitale account op een vertrouwelijke manier is gekoppeld aan een reële identiteit, geverifieerd door een erkende betrouwbare derde partij.

Een dergelijk systeem bestaat al in andere domeinen van het dagelijks leven. In het verkeer zijn we identificeerbaar aan de hand van onze nummerplaat, zonder dat onze naam op onze auto staat. Wanneer een burger een elektronische handtekening gebruikt via een tool zoals Itsme, wordt zijn identiteit voor echt verklaard door een tussenpersoon, zonder dat die informatie wordt verspreid. Dat model van geverifieerde pseudonimiteit, dat de persoonlijke levenssfeer in acht neemt en tegelijk een mogelijke verantwoordelijkheid waarborgt, kan en moet worden omgezet in beschermende regels die van toepassing zijn op de wereld van de sociale media.

Het is niet de bedoeling een welbepaalde oplossing op te leggen en nog minder om de platformen de persoonlijke gegevens van de burgers te bezorgen. Het komt erop neer een architectuur te ontwerpen waarbinnen in het volste vertrouwen de verificatie van de identiteit wordt uitbesteed, beveiligd, geregeld en alleen raadpleegbaar is door een uitspraak van de rechter. Binnen dat systeem kan iedereen blijven interageren onder een pseudoniem, maar weet iedereen ook dat bij illegaal gedrag identificatie mogelijk is. Dat perspectief is allesbehalve een aanslag op de vrijheid, maar werkt ontvoogdend; het beschermt de slachtoffers, ontmoedigt misbruik, versterkt de nettiquette en maakt de digitale ruimte geloofwaardig omdat die aldus uitgroeit tot een echte democratische ruimte.

ne protège pas les faibles, il protège les agresseurs. Il ne favorise pas le débat, il le disloque. Il ne garantit pas la liberté d'expression, il en dégrade le sens et la portée.

Une démocratie adulte ne peut pas tolérer que l'espace public numérique échappe à toute forme de responsabilité. Elle ne peut pas accepter que les victimes doivent choisir entre le silence ou l'exposition publique de leur souffrance, sans aucun recours effectif contre leurs agresseurs. Elle ne peut pas continuer à subir, sur ses propres territoires, les conséquences d'un modèle d'interactions conçu ailleurs, sans transparence, sans équité, sans règles claires.

Il est donc temps d'ouvrir un chantier politique de grande ampleur, celui de la responsabilité individuelle des acteurs du numérique, fondée non pas sur la surveillance généralisée ou l'abolition de la vie privée mais sur la possibilité concrète, garantie légalement, de pouvoir identifier l'auteur d'un abus en ligne lorsque la loi l'exige. Ce chantier ne consiste pas à exiger que chacun publie sous son nom; il consiste à créer un système où chaque compte numérique est lié, de manière confidentielle, à une identité réelle, vérifiée par un tiers de confiance agréé.

Un tel système existe déjà dans d'autres domaines de la vie quotidienne. Lorsque nous circulons sur la voie publique, nous sommes identifiables via notre plaque d'immatriculation, sans que notre nom soit affiché sur notre voiture. Lorsqu'un citoyen utilise une signature électronique via un outil comme Itsme, son identité est certifiée par un intermédiaire, sans que cette information soit diffusée. Ce modèle de pseudonymat vérifié, respectueux de la vie privée tout en étant garant d'une responsabilité potentielle peut, et doit, être transposé dans des règles protectrices applicables à l'univers des réseaux sociaux.

Il ne s'agit pas d'imposer une solution unique, encore moins de livrer aux plateformes les données personnelles des citoyens. Il s'agit d'imaginer une architecture permettant de garantir la confiance dans laquelle la vérification de l'identité est externalisée, sécurisée, encadrée et consultable uniquement par décision judiciaire. Dans ce système, chacun peut continuer à interagir sous pseudonyme mais sait que, en cas de comportement illégal, il pourra être identifié. Cette perspective, loin d'être liberticide, est émancipatrice; elle protège les victimes, décourage les abus, renforce la civilité, crédibilise l'espace numérique en lui permettant d'être un réel espace démocratique.

De Belgische Staat beschikt over de technische en institutionele capaciteit om een dergelijk model te implementeren. Hij kan gebruikmaken van de bestaande infrastructuren, van de expertise van zijn overheidsinstellingen en van een duidelijk juridisch raamwerk. Maar naast capaciteit is er vandaag ook politieke wil nodig. Weigeren de anonimiteitskwestie frontaal aan te pakken betekent dat het aan de digitale reuzen wordt overgelaten om de grenzen van onze publieke ruimte vast te leggen. Zulks betekent afstand doen van onze democratie.

Het doel van dit eerste hoofdstuk is niet álle problemen op te lossen of álle hangijzers te beslechten, maar alvast deze vereiste te bevestigen: de rechtsstaat moet integraal zijn. Hij mag niet stoppen waar het internet begint. Als we de democratie willen beschermen, moeten we garanderen dat de beginselen ervan ook gelden in de digitale wereld.

2. ***Minderjarigen online: geen afdoende bescherming en leeftijdscontrole***

Onze wereld is steeds meer gedigitaliseerd. Kinderen en adolescenten spelen een centrale rol in de door de communicatietechnologieën gecreëerde dynamieken. Ze groeien op in de geconnecteerde omgeving die is uitgebouwd rond platformen, die richting geven aan hun sociale interacties, vrijetijdsactiviteiten en identiteitsvorming. Die massale online aanwezigheid van minderjarigen is een maatschappelijk fenomeen dat zich al even snel als diep heeft verankerd. De regulering van die online ruimte loopt echter schromelijk achter, vooral op het vlak van de bescherming van minderjarigen tegen risico's die inherent zijn aan digitale omgevingen en inzonderheid sociale media.

Net als in de meeste andere Europese landen bestaat er in België vooralsnog geen degelijk, betrouwbaar en veralgemeend systeem om effectief de leeftijd te controleren van wie tot de sociale platformen toegang heeft. De meeste grote platformen hanteren een willekeurige minimumleeftijd (soms 13 jaar, soms 16, naargelang van de functie). De controle op die leeftijd is echter louter gebaseerd op een verklaring van de gebruiker: met een simpele klik en een valse geboortedatum kan men dat obstakel immers gemakkelijk omzeilen. Daardoor ontstaat de absurde situatie dat de wet niet wordt nageleefd gewoon omdat er geen controlemechanisme is.

Belgische kinderen (soms niet ouder dan 9 of 10) zijn dus massaal aanwezig op voor volwassenen ontworpen platformen, waarvan de modereringslogica amper op hun kwetsbaarheid is toegesneden en waar zonder enige filter mechanismen spelen die verslavingsgedrag, algoritmegedreven verzoeken en persoonsgegevensopslag

L'État belge a la capacité technique et institutionnelle de mettre en œuvre un tel modèle. Il peut s'appuyer sur les infrastructures existantes, sur l'expertise de ses organes publics, sur un cadre juridique clair. Mais, au-delà de la capacité, il faut aujourd'hui la volonté politique. Refuser d'aborder frontalement la question de l'anonymat revient à abandonner aux géants du numérique le soin de fixer les limites de notre espace public. C'est une démission de notre démocratie.

Ce premier chapitre de la réflexion ne vise pas à résoudre tous les problèmes ni à trancher toutes les questions débattues; il vise à affirmer une exigence; l'État de droit doit être intégral. Il ne peut pas s'arrêter là où commence Internet. Si nous voulons protéger la démocratie, nous devons garantir que ses principes s'appliquent aussi dans l'univers numérique.

2. ***Mineurs en ligne, une protection contournée, un âge ignoré***

Dans un monde de plus en plus numérisé, les enfants et les adolescents occupent une place centrale dans les dynamiques d'usage des technologies de communication. Ils grandissent dans un environnement connecté, façonné par des plateformes qui rythment leurs interactions sociales, leurs loisirs, leur construction identitaire. Cette présence massive des mineurs dans l'univers numérique constitue un phénomène social aussi profond que rapide. Pourtant, la régulation de cet espace reste cruellement en retard, notamment en ce qui concerne la protection des mineurs contre les risques propres à l'environnement numérique, en particulier sur les réseaux sociaux.

Aujourd'hui, en Belgique comme dans la plupart des États européens, aucun système solide, fiable et généralisé ne garantit un contrôle effectif de l'âge pour l'accès aux plateformes sociales. La majorité des grandes plateformes fixent arbitrairement l'âge minimum à 13 ans, parfois 16 pour certaines fonctions. Ces limites d'âge sont cependant purement déclaratives; un simple clic, une fausse date de naissance et l'obstacle est ainsi facilement contourné. Il en résulte une situation absurde où la loi n'est pas respectée à cause de l'absence de tout mécanisme de vérification.

Les enfants belges (parfois dès l'âge de 9 ou 10 ans) sont donc massivement présents sur des plateformes conçues pour des adultes, où les logiques de modération sont peu adaptées à leur vulnérabilité, et où les mécanismes d'addiction comportementale, de sollicitation algorithmique ou de captation de données personnelles

in de hand werken. In werkelijkheid ontbreekt het aan echte voorzorgsmaatregelen om te voorkomen dat kinderen zich op sociale media registreren of om de digitale ervaring op hun werkelijke leeftijd af te stemmen.

Het is een welbekende situatie, waar ook al veel onderzoek naar is gedaan. Al jaren waarschuwen kinderbeschermingsorganisaties, onderzoekers, organisaties uit het veld en gezinnen voor het ontbreken van echte barrières die voorkomen dat minderjarigen toegang krijgen tot toxische inhoud: haatspraak, seksueel getinte inhoud, risicovol schoonheids- of voedingsadvies, seksueel getinte verzoeken, risico-uitdagingen die viraal gaan of blootstelling aan niet-gewenste boodschappen. Zowel Belgisch als internationaal onderzoek toont aan dat dergelijke vroegtijdige, niet-begeleide online aanwezigheid een rechtstreeks effect heeft op de mentale gezondheid van de jongeren, hun gevoel van eigenwaarde, hun slaap en hun schoolresultaten. Tegelijk zijn ze vatbaarder voor risicogedrag en kwetsbaarder voor misbruik.

Volgens onderzoek van Child Focus en Média Animation heeft in België bijna 70 % van de kinderen tussen 11 en 13 jaar al minstens één socialemediaprofiel. Bij 14-15-jarigen stijgt dat percentage tot meer dan 90 %. Uit het onderzoek blijkt tevens dat de meesten bij het aanmaken van die account over hun leeftijd hebben gelogen, vaak oogluikend toegelaten door de omgeving. Het betreft hier dan ook geen uitzonderingssituatie maar een massaverschijnsel, dat in een grijze zone kan gedijen omdat de platformen er geen graten in zien en de wetgever het ongemoeid laat.

Die discrepantie tussen het werkelijke online gedrag van minderjarigen en de wettelijke regulering heeft een dubbel neveneffect. Enerzijds blijven minderjarigen verstoken van een specifieke bescherming wanneer ze inloggen op platformen waarvan de mechanismen totaal niet aan hun leeftijd zijn aangepast. Anderzijds staan ouders, opvoeders, leerkrachten, sociale of gerechtelijke diensten machteloos wanneer ze te maken krijgen met kinderen en jongeren die afzien, gepest worden of verslaafd geraken; ze kunnen immers niets doen aan de oorzaak van het probleem.

Cyberpesten op school is een voorbeeld bij uitstek. Wanneer een leerling een andere leerling lastigvalt via een anonieme account of een privégroep op een sociaal platform, is het voor de schooldirectie, de ouders en soms zelfs voor de politie zeer moeilijk om de verantwoordelijken te identificeren, de feiten een halt toe te roepen of gewoon de medewerking van het platform te krijgen. Dat vacuüm in de regelgeving voedt en versterkt het al eerder genoemde gevoel van straffeloosheid. Daarenboven zijn de jongeren extra kwetsbaar omdat ze zich nog in hun kindertijd bevinden.

s'exercent sans filtre. Dans les faits, aucun garde-fou véritable n'est en place pour empêcher l'inscription d'un enfant sur un réseau social, ni pour adapter l'expérience numérique à son âge réel.

Cette situation est connue et documentée. Depuis des années, les organisations de protection de l'enfance, les chercheurs, les associations de terrain, les familles alertent sur l'absence de barrière réelle empêchant les mineurs d'accéder à des contenus toxiques: discours haineux, contenus sexualisés, injonctions esthétiques ou alimentaires dangereuses, sollicitations sexuelles, défis viraux à risque, exposition non désirée. Les études, tant belges qu'internationales, pointent un effet direct de ces usages précoces et non encadrés sur la santé mentale des jeunes, leur estime de soi, leur sommeil, leurs résultats scolaires, leur exposition à des comportements à risque, voire à des situations d'abus.

En Belgique, selon une enquête menée par Child Focus et Média Animation, près de 70 % des jeunes de 11 à 13 ans disposent déjà d'au moins un compte sur un réseau social. Ce chiffre grimpe à plus de 90 % pour les 14-15 ans. L'étude révèle également que la majorité d'entre eux ont menti sur leur âge pour créer ce compte, souvent avec la complicité passive de l'entourage. Il ne s'agit donc pas d'exceptions mais d'un phénomène de masse. Et ce phénomène évolue dans une zone de flou, à la fois toléré par les plateformes et ignoré par le législateur.

Ce décalage entre les usages réels des mineurs et la régulation légale produit un double effet pervers. D'une part, les mineurs ne bénéficient d'aucune protection spécifique sur des plateformes dont les mécanismes sont profondément inadaptés à leur âge. D'autre part, les parents, éducateurs, enseignants, services sociaux ou judiciaires se retrouvent démunis face à des situations de souffrance, de harcèlement ou de dépendance, faute de pouvoir agir sur la cause à l'origine du problème.

Le cas du cyberharcèlement scolaire est particulièrement emblématique. Lorsqu'un élève harcèle un autre via un compte anonyme ou un groupe privé sur une plateforme sociale, les directions d'école, les parents et parfois même les autorités policières rencontrent des obstacles considérables pour identifier les responsables, faire cesser les faits, ou simplement obtenir la coopération de la plateforme. Ce vide réglementaire alimente et amplifie le sentiment d'impunité déjà évoqué; cela, dans un contexte où des jeunes se trouvent dans des situations particulièrement fragiles, durant l'enfance.

Die gebrekkige leeftijdscontrole staat bovendien elke vorm van gestructureerde bewustmaking in de weg. Zolang platformen geen echte zekerheid hebben over de leeftijd van hun gebruikers, kunnen (of willen) ze hun interface, inhoud, aanbevelingssysteem of reclamestrategie niet bijsturen. Ze zijn niet bij machte om met gepaste striktheid de toegang tot bepaalde inhoud in te perken, noch getrapte rechten in te bouwen voor aangepaste toegang tot de desbetreffende functies, zoals dat wel al gebeurt in andere sectoren waar de kwetsbaarheid van minderjarigen in het spel is (videospelen, reclame, audiovisuele content).

Nochtans is het perfect mogelijk een evoluerende digitale ervaring te concipiëren op maat van elke leeftijdscategorie, aan de hand van een logica van getrapte toegang, responsabilisering, gegevensbescherming en psychosociale ontwikkeling. Dat voornemen wordt echter gefnuikt door een obstakel van formaat: de onzekerheid over hoe oud iemand werkelijk is. De ingevulde leeftijd is in wezen waardeloos, aangezien de platformen over geen enkel gedegen leeftijdsverificatiemechanisme beschikken.

In andere gevoelige sectoren (alcoholverkoop, gokspelen, rijbewijs, onderwijs) is de leeftijd een essentieel, geverifieerd, gecontroleerd en tegenstelbaar criterium. Waarom zou dat anders mogen zijn in de digitale wereld, die een even grote of misschien zelfs grotere invloed uitoefent dan al die andere sectoren samen? Waarom zou de leeftijd een omzeilbare formaliteit mogen zijn in een omgeving van mondiale interactie die wordt geregeerd door algoritmen, commerciële belangen en uitermate intense sociale dynamieken?

Het vaak aangehaalde technische argument, met name dat het te moeilijk is om iemands leeftijd te verifiëren zonder diens privacy te schenden, houdt eigenlijk geen steek. Er bestaan vandaag immers concrete, technisch beproefde en juridisch regelbare middelen om de werkelijke leeftijd van een gebruiker na te gaan zonder diens identiteit prijs te geven. Betrouwbare digitale derden, naar het voorbeeld van de Belgische Itsme-app, zijn in staat te bevestigen dat een individu wel degelijk een bepaalde leeftijd heeft zonder aanvullende informatie vrij te geven. Die logica, die al bij talloze administratieve, bank- of contractuele verrichtingen gebruikelijk is, zou kunnen worden toegepast bij de registratie op sociale media of bij de activering van bepaalde gevoelige functies. De Europese Commissie is ook gestart met het proefproject White Label App, dat net tot doel heeft een systeem voor leeftijdsverificatie van de gebruikers uit te werken dat verenigbaar is met het Europese regelgevende kader.

Ce manque de contrôle de l'âge empêche également toute politique éducative structurée. Tant que les plateformes n'ont pas la garantie de l'âge de leurs utilisateurs, elles ne peuvent (ou ne veulent) pas adapter leur interface, leur contenu, leur système de recommandation ou leur politique de publicité. Elles ne peuvent pas, avec la rigueur voulue, limiter l'accès à certains types de contenus ni instaurer des paliers progressifs pour un accès adapté aux fonctionnalités concernées, comme c'est le cas dans d'autres secteurs exposés à la vulnérabilité des mineurs (jeux vidéo, publicité, contenus audiovisuels).

Il serait pourtant tout à fait possible de concevoir une expérience numérique évolutive, adaptée à chaque tranche d'âge, sur la base de principes de progressivité, de responsabilisation, de protection des données et de développement psycho-social. Mais cette perspective est aujourd'hui bloquée par une difficulté majeure; on ne sait pas qui a quel âge. La donnée déclarée n'a aucune valeur car les plateformes ne disposent d'aucun mécanisme sérieux pour vérifier cette information.

Dans d'autres secteurs sensibles (vente d'alcool, jeux d'argent, permis de conduire, scolarité) l'âge est un critère fondamental, vérifié, contrôlé, opposable. Pourquoi en serait-il autrement dans l'univers numérique, qui exerce une influence aussi massive, sinon plus, que tous ces secteurs réunis? Pourquoi l'âge serait-il une formalité contournable lorsqu'il s'agit de pénétrer un espace d'interactions mondialisées, régi par des algorithmes, des intérêts commerciaux et des dynamiques sociales à haute intensité?

Concernant l'argument technique souvent invoqué (il serait trop difficile de vérifier l'âge sans porter atteinte à la vie privée) l'absence de pertinence mérite d'être soulignée. Car il existe aujourd'hui des moyens concrets, techniquement éprouvés et juridiquement encadrables, pour garantir l'âge réel d'un utilisateur sans exposer publiquement son identité. Des tiers de confiance numériques, à l'instar de ce que permet déjà l'application Itsme en Belgique, sont capables de confirmer qu'un individu a bien atteint un certain âge sans divulguer aucune information supplémentaire. Cette logique, déjà appliquée dans de nombreuses démarches administratives, bancaires ou contractuelles, pourrait être transposée à l'inscription sur les réseaux sociaux ou à l'activation de certaines fonctionnalités sensibles. La Commission européenne conduit également un projet pilote "White Label App" dont l'objet est précisément de proposer une solution de vérification de l'âge des utilisateurs compatible avec le cadre juridique européen.

Zulke oplossing zou de handhaving van de minimumleeftijd niet alleen werkzamer maken, maar tevens het pad effenen voor doeltreffendere vormen van wat men “digitaal ouderschap” noemt. Dat maakt de ontwikkeling mogelijk van geloofwaardige, geverifieerde systemen voor ouderlijke toestemming, getrapte autonomieniveaus en fora voor bemiddeling of voor intergenerationele dialoog; andermaal op voorwaarde natuurlijk dat de ingevulde leeftijd betrouwbaar is.

Het gaat er niet om een maatschappij te creëren waarin minderjarigen constant worden gemonitord, noch om gezinnen te ontslaan van hun opvoedkundige taak. Het komt erop aan de minimale voorwaarden voor een verantwoordelijk raamwerk te scheppen, waarbinnen overheidsinstellingen hun beschermingsplicht kunnen vervullen zonder die opdracht volledig uit te besteden aan particuliere commerciële ondernemingen.

In dat opzicht zou België niet alleen zijn scala aan kinderbeschermingsinstrumenten kunnen verbreden maar ook actief bijdragen tot een Europese denkoefening over de voorwaarden om minderjarigen toegang te geven tot digitale toepassingen. Sinds in landen zoals Frankrijk overleg is gestart over wetgeving tot invoering van een leeftijdsgrens voor de toegang tot sociale media of tot identiteitsverificatie bij de registratie, kan België niet achterblijven. Ons land beschikt over de technische instrumenten, instellingen en expertise om een voortrekkersrol te spelen in de uitrol van realistische regelgeving die tegelijk de rechten eerbiedigt en vasthoudt aan de nodige principes.

De Kamer van volksvertegenwoordigers draagt de verantwoordelijkheid dit vraagstuk scherpzinnig en vastberaden aan te pakken. Het is niet de bedoeling jongeren met de vinger te wijzen over hun digitale gewoonten of te dromen van een “gouden leeftijd zonder schermpjes”. Het gaat erom een samenhangend, evenredig en beschermend raamwerk te scheppen dat de specifieke aard van kinderen in de digitale wereld erkent en daar ook oog voor heeft zonder dat deze of gene marktlogica de bovenhand haalt of men alles maar op zijn beloop laat.

De uitdaging is zowel eenvoudig als immens: een einde maken aan de ontkenning, de onverschilligheid of de hypocrisie omtrent het gebruik van sociale media door minderjarigen, maar kiezen voor een logica van transparantie, veiligheid en gedeelde verantwoordelijkheid. Dat noopt tot een duidelijke keuze: een einde maken aan de gekoesterde illusies van een bepaalde opgegeven leeftijd en een systematische leeftijdsverificatie instellen bij registratie op sociale media. Een verificatie die afgebakend, onafhankelijk, technologisch robuust en privacybestendig is.

Adopter cette solution permettrait non seulement de rendre effectif le respect de l’âge minimum d’accès mais également d’ouvrir la voie à des formes de parentalité numérique plus efficaces. Des mécanismes d’autorisation parentale vérifiés, des paliers d’autonomie progressifs, des espaces de médiation ou de dialogue intergénérationnels pourraient alors être développés de manière crédible; à condition, encore une fois, que la donnée relative à l’âge soit fiable.

Il ne s’agit pas de créer une société de surveillance des mineurs ni de déposséder les familles de leur rôle éducatif. Il s’agit de créer les conditions minimales d’un encadrement responsable, dans lequel les institutions publiques assument leur devoir de protection sans déléguer entièrement cette mission à des entreprises privées à vocation commerciale.

Dans cette perspective, la Belgique pourrait non seulement renforcer son arsenal de protection de l’enfance mais également contribuer activement à une réflexion européenne sur les conditions d’accès des mineurs aux environnements numériques. Alors que plusieurs pays, comme la France, ont amorcé des discussions au niveau législatif sur l’interdiction de l’accès aux réseaux sociaux avant un certain âge ou sur la vérification de l’identité à l’inscription, la Belgique ne peut rester en retrait. Elle dispose des outils techniques, des institutions, de l’expertise pour jouer un rôle moteur dans la mise en place d’une régulation réaliste, respectueuse des droits, mais ferme sur les principes.

La Chambre des représentants a la responsabilité de se saisir de cette question avec lucidité et détermination. Il ne s’agit pas de moraliser les usages numériques des jeunes, ni de fantasmer un âge d’or sans écrans. Il s’agit de construire un cadre cohérent, proportionné, protecteur, qui reconnaît la spécificité de l’enfance dans l’environnement numérique et qui garantit que cette spécificité soit bien respectée sans que les logiques de marché ou le laisser-faire prennent le dessus.

L’enjeu est à la fois simple et immense, garantir que l’accès des mineurs aux réseaux sociaux ne se fasse plus dans le déni, dans le contournement ou dans l’hypocrisie, mais dans la transparence, la sécurité et la responsabilité partagée. Cela implique de faire un choix clair; celui de mettre fin à l’illusion d’un âge déclaré et d’instaurer une vérification systématique de l’âge à l’entrée des réseaux sociaux. Une vérification encadrée, indépendante, technologiquement robuste et respectueuse de la vie privée.

België heeft die keuze. Ons land moet dit vraagstuk beschouwen als een hoeksteen van de democratie, net zoals onderwijs, gezondheid of veiligheid. In de wereld van vandaag en morgen betekent minderjarigen beschermen ook hen online beschermen.

3. ***Digitaal geweld gedijt bij straffeloosheid***

Sociale media en digitale communicatieplatformen zijn uitgegroeid tot hotspots van hedendaagse discoursen. Het zijn ruimtes voor debat, informatie, mobilisatie en contestatie, maar ook ruimtes waar geweld bijzonder intens, zichtbaar en ongemeen snel tot uiting komt. Dergelijk geweld is allesbehalve een randverschijnsel of uitzondering, maar zit ingebakken in de wijze waarop digitale omgevingen werken. Het heeft echter zelden gevolgen voor de daders. Het gedijt in straffeloosheid.

Online geweld neemt uiteenlopende vormen aan. Het kan verbaal, psychologisch, seksueel, symbolisch of economisch van aard zijn. Het uit zich via beledigingen, bedreigingen, belaging, lastercampagnes, haatdiscoursen of gerichte publieke vernedering. Het kan gericht zijn tegen een individu, een categorie van mensen of een gemeenschap. Het kan het werk zijn van een enkeling, een gecoördineerde groep of een schimmig, ongeorganiseerd geheel.

In tegenstelling tot fysiek geweld is digitaal geweld immaterieel, veelvuldig, persistent en vaak onzichtbaar voor degenen die het zelf niet moeten ondergaan. Het houdt geen rekening met grenzen of afstand en wordt de klok rond herhaald. Het wordt versterkt doordat het gedeeld en becommentarieerd wordt en onderworpen is aan algoritmen. Het treedt de intieme sfeer binnen. Het wordt opgeslagen in digitale geheugens en verdwijnt nooit.

Het treft heel uiteenlopende groepen, maar op ongelijke wijze. Uit studies blijkt dat dergelijk geweld zich in het bijzonder richt tegen vrouwen, jongeren, lgbtqia+'ers, mensen van kleur, journalisten, verkozenen, onderwijzers, activisten of kwetsbare personen. Cyberpesten op school, digitale raids, vrouwonvriendelijke of racistische discoursen, bedreigingen aan het adres van onderzoeksjournalisten of verkozenen zijn schering en inslag geworden, worden gebagatelliseerd of zijn kennelijk soms zelfs gewoon een "risico van het vak".

Dergelijk digitaal geweld berokkent niet alleen individueel leed. Het heeft ook collectieve en systemische effecten. Het dwingt mensen ertoe zich terug te trekken uit het publieke debat, aan zelfcensuur te doen, hun baan op te zeggen of de digitale ruimte te ontvluchten. Het tast de kwaliteit van de democratische dialoog aan,

Ce choix, la Belgique peut le faire. Elle doit même l'envisager comme une exigence démocratique, au même titre que l'école, la santé ou la sécurité. Car, dans le monde actuel et futur, protéger les mineurs, c'est aussi les protéger en ligne.

3. ***La violence numérique prospère dans l'impunité***

Les réseaux sociaux et les plateformes de communication numérique sont devenus les principaux lieux de projection de la parole contemporaine. Ce sont des espaces de débat, d'information, de mobilisation, de contestation (mais aussi des espaces où la violence s'exprime avec une intensité, une visibilité et une rapidité inédite). Une violence qui, loin d'être marginale ou exceptionnelle, s'inscrit dans le fonctionnement quotidien des environnements numériques. Or, cette violence est rarement suivie de conséquences pour leurs auteurs. Elle prospère dans l'impunité.

La violence en ligne prend des formes variées. Elle peut être verbale, psychologique, sexuelle, symbolique ou économique. Elle s'exprime par des insultes, des menaces, du harcèlement répété, des campagnes de diffamation, des discours de haine ou encore l'humiliation publique ciblée. Elle peut viser un individu, une catégorie de personnes, une communauté. Et elle peut être exercée par un individu isolé, un groupe coordonné ou un ensemble diffus et désorganisé.

Contrairement à la violence physique, la violence numérique est désincarnée, démultipliée, persistante et souvent invisible pour ceux qui ne la subissent pas. Elle franchit les frontières, efface la distance, se répète 24 heures sur 24, est amplifiée par les partages, les commentaires, les algorithmes. Elle envahit la sphère intime. Elle s'archive dans les mémoires numériques; elle ne disparaît jamais.

Elle touche des publics très divers mais de manière inégale. Les études montrent que les femmes, les jeunes, les personnes LGBTQIA+, les personnes racisées, les journalistes, les élus, les enseignants, les activistes ou les personnes en situation de vulnérabilité sont particulièrement ciblés. Le cyberharcèlement scolaire, les raids numériques, les discours misogynes ou racistes, les menaces contre les journalistes d'investigation ou les élus sont devenus des réalités courantes, banalisées, parfois même intégrées comme un "risque du métier".

Cette violence numérique ne produit pas que des souffrances individuelles. Elle a des effets collectifs et systémiques. Elle pousse des personnes à se retirer du débat public, à censurer leur parole, à quitter leur métier, à fuir l'espace numérique. Elle altère la qualité du dialogue démocratique, polarise les positions, dégrade

polariseert standpunten, ondermijnt het vertrouwen en werkt radicalisering in de hand. Het voedt cynisme en het gevoel van ontreddering. Het verzwakt instellingen en versterkt een logica waarin mensen zich op zichzelf gaan terugplooien of haat gaan koesteren.

Ondanks de omvang van dit geweld blijft het grotendeels onbestraft. Er bestaan weliswaar straf-, burger- en bestuursrechtelijke mechanismen, maar er zijn veel obstakels. Het identificeren van de daders is moeilijk, een klacht indienen is complex en een gerechtelijk antwoord komt er veelal pas na een lang, onzeker en uitputtend proces. De slachtoffers van digitaal geweld voelen zich compleet aan hun lot overgelaten na alles wat ze concreet hebben ervaren: er wordt niets ondernomen, hun klacht draait op niets uit en de instellingen hullen zich in stilzwijgen. Het is een vicieuze cirkel: hoe meer straffeloosheid als onvermijdelijk wordt gezien, hoe meer het geweld legitiem of althans aanvaardbaar wordt.

De digitale platformen beweren die fenomenen tegen te gaan. Ze wijzen op hun gedragscodes, moderatiebeleid en meldingsinstrumenten. Die middelen zijn echter ontoereikend, ondoorzichtig en onsamenhangend. De criteria voor het modereren variëren naargelang van de taal, de context en het land. De antwoorden zijn geautomatiseerd, onpersoonlijk en willekeurig. Er wordt niet effectief opgetreden. De gemelde gebruiker kan gewoon een nieuwe account aanmaken. De geschorste account kan weer opduiken in een andere vorm. Collectieve belaging kan ook in privégroepen plaatsvinden, zonder zichtbare sporen. Problematische accounts kunnen blijven gedijen zolang ze genoeg succes hebben.

Deze situatie plaatst de slachtoffers voor een wrede paradox: ze worden publiekelijk blootgesteld aan reëel geweld, maar kunnen er niet effectief op reageren of zich zonder schade terugtrekken. Een platform verlaten betekent immers dat men een ruimte voor sociale verbinding, professionele zichtbaarheid en burgerparticipatie verliest. Voor verkozenen, journalisten, activisten, kunstenaars, onderwijzers of adolescenten is uit een groep stappen niet langer een neutrale optie.

Digitale straffeloosheid is ook het resultaat van een structurele discrepantie tussen het tijdsaspect van online geweld (snel, viraal, onmiddellijk) en dat van de gerechtelijke of politionele instellingen (langzaam, behoedzaam, formeel). Wanneer een slachtoffer van belaging een klacht indient, staat de politie vaak machteloos: gebrek aan opleiding, geen gespecialiseerde eenheid, obstakels bij het voeren van het onderzoek, afhankelijkheid van de platformen, complexiteit van het internationaal privaatrecht. Tal van zaken worden niet

la confiance, favorise la radicalisation. Elle nourrit le cynisme et le sentiment d'abandon. Elle fragilise les institutions et alimente les logiques de repli ou de haine.

Or, malgré son ampleur, cette violence reste très largement impunie. Les mécanismes juridiques existent (en droit pénal, civil ou administratif) mais les obstacles sont nombreux. Identifier les auteurs est difficile, déposer plainte est complexe, obtenir une réponse judiciaire nécessite un processus long, incertain et épuisant. Le sentiment d'abandon que ressentent les victimes de violences numériques est profond; il est causé par des expériences concrètes d'inaction, de non-lieu, de silences institutionnels. C'est un cercle vicieux; plus l'impunité est perçue comme inévitable, plus la violence devient légitime, ou du moins tolérable.

Les plateformes numériques affirment lutter contre ces phénomènes. Elles mettent en avant leurs chartes de bonne conduite, leurs politiques de modération, leurs outils de signalement. Mais ces dispositifs sont insuffisants, opaques et incohérents. Les critères de modération varient selon les langues, les contextes, les pays. Les réponses sont automatisées, impersonnelles, aléatoires. Il n'y a pas de recours effectif. L'utilisateur signalé peut simplement ouvrir un nouveau compte. Le compte suspendu peut réapparaître sous une autre forme. L'organisation d'un harcèlement collectif peut se faire dans des groupes privés, sans trace visible. Les comptes problématiques peuvent continuer à prospérer, tant qu'ils génèrent de l'engagement.

Cette situation place les victimes dans un situation paradoxale cruelle; elles sont exposées publiquement à une violence réelle, mais elles ne peuvent ni y répondre efficacement, ni se retirer sans dommage. Car quitter les plateformes signifie aussi perdre un espace de sociabilité, de visibilité professionnelle, de participation citoyenne. Pour un élu, un journaliste, un militant, un artiste, un enseignant ou un adolescent, se déconnecter n'est plus une option neutre.

L'impunité numérique résulte également d'un décalage structurel entre la temporalité de la violence en ligne (rapide, virale, immédiate) et celle des institutions judiciaires ou policières (lente, prudente, formelle). Lorsqu'une victime de harcèlement porte plainte, les forces de l'ordre sont souvent démunies; manque de formation, absence de cellule spécialisée, difficultés pour mener l'enquête, dépendance aux plateformes, complexité du droit international privé. Dans de nombreux cas, aucune suite n'est donnée. Et, même lorsque

vervolgd. Zelfs wanneer de procedure wordt volbracht, komt het zelden tot een sanctie, ofwel komt die te laat of is ze louter symbolisch.

Dat probleem doet zich niet alleen in België voor. Het gaat om een gedeelde vaststelling in heel wat democratieën, waar de instellingen er ternauwernood in slagen hun instrumenten aan het nieuwe informatie-ecosysteem aan te passen. Die vaststelling mag echter niet tot berusting leiden. Integendeel, ze vraagt om een grondige herziening van onze aanpak van online geweld. Dat geweld is immers geen uitzondering meer, maar is structureel geworden. Misbruik is geen marginaal verschijnsel; het is een symptoom van onze falende regelgeving.

Geweld gedijt onder meer omdat de dader er geen enkele prijs voor hoeft te betalen; geen filter, geen verantwoordelijkheid, geen reëel risico om geïdentificeerd of bestraft te worden. De dader van een haatbericht, doodsbedreiging, vernederende montage of gecoördineerde aanval handelt vaak vanaf een anonieme account, in luttele seconden aangemaakt vanaf een verborgen IP-adres. Hij weet dat de kans om vervolgd te worden miniem is. Die asymmetrie tussen het gemak waarmee schade kan worden berokkend en de moeilijkheid om zich te verdedigen is op lange termijn onhoudbaar voor een democratische samenleving.

Meer zelfs, dergelijke digitale straffeloosheid creëert een vorm van hiërarchie tussen burgers. Sommige mensen (omdat ze in de kijker lopen, kwetsbaar of minderjarig zijn) worden blootgesteld aan geweld, terwijl anderen (die de codes, de tools, de pseudoniemen beheersen) kunnen uithalen zonder voor gevolgen te hoeven vrezen. Dat is een schending van de gelijkheid voor de wet. Het is een breuk in de maatschappelijke orde omdat de belofte van bescherming van elke burger niet wordt nagekomen.

Staten moeten die situatie van straffeloosheid erkennen als wat ze echt is: een lacune in hun soevereiniteit; een onvermogen om de wet te handhaven in een ruimte waar een steeds groter deel van het gemeenschapsleven zich afspeelt. Dit voorstel van resolutie roept niet op tot algemene repressie of verscherpt toezicht. Het vraagt mogelijk te maken wat vandaag onmogelijk is: daders identificeren, feiten vaststellen en de wet handhaven. Zonder die capaciteit blijft de wetsnorm niet meer dan symboliek en wordt de democratie ondermijnd.

Daarom moet op een heldere manier worden gesproken over identificatie, verantwoordelijkheid en het beëindigen van de digitale straffeloosheid. Dat is geen autoritaire uitwas, maar een eis voor rechtvaardigheid; geen emotionele reactie op individuele tragedies, maar een structurele, proportionele en legitieme regulerende

la procédure aboutit, les sanctions sont rares, tardives, symboliques.

Ce constat n'est pas propre à la Belgique. Il est partagé par de nombreuses personnes dans de nombreuses démocraties où les institutions peinent à adapter leurs outils au nouvel écosystème informationnel. Mais ce constat ne doit pas conduire à la résignation. Il appelle au contraire à une révision profonde de notre approche de la violence en ligne. Car celle-ci n'est pas une exception; elle est devenue structurelle. Les abus ne sont pas des phénomènes marginaux; ils sont un symptôme de notre modèle de régulation défaillant.

Cette violence prospère notamment parce qu'elle ne coûte rien à celui qui l'exerce. Aucun filtre, aucune responsabilité, aucun risque réel d'être identifié ou sanctionné. L'auteur d'un commentaire haineux, d'une menace de mort, d'un montage humiliant ou d'un raid coordonné agit souvent depuis un compte anonyme, créé en quelques secondes, depuis une adresse IP dissimulée. Il sait que la probabilité d'être poursuivi est infime. Cette asymétrie entre la facilité de nuire et la difficulté de se défendre est intenable à long terme pour une société démocratique.

Plus encore, cette impunité numérique crée une forme de hiérarchie entre les citoyens. Certains (parce qu'ils sont visibles, vulnérables, minorisés) sont exposés à la violence. D'autres (parce qu'ils maîtrisent les codes, les outils, les pseudonymes) peuvent agresser sans craindre les conséquences. C'est une rupture d'égalité devant la loi. C'est une fracture de l'ordre social car la promesse de la protection pour tous n'est pas respectée.

Les États doivent reconnaître cette situation d'impunité pour ce qu'elle est; une faille dans leur souveraineté. Une incapacité à faire respecter le droit dans un espace où se joue une part croissante de la vie collective. Il ne s'agit pas de réclamer une répression généralisée, ni d'étendre la surveillance. Il s'agit de rendre possible ce qui est aujourd'hui empêché; identifier un auteur, établir un fait, appliquer la loi. Sans cette capacité, la norme juridique reste symbolique. Et la démocratie se trouve fragilisée.

C'est pourquoi la réflexion sur l'identification, la responsabilité et la fin de l'impunité numérique doit être menée avec clarté. Non pas comme une dérive autoritaire mais comme une exigence de justice. Non pas comme une réponse émotionnelle à des drames isolés mais comme une mesure de régulation structurelle, proportionnée et

maatregel. Het doel is niet om de vrijheid van meningsuiting in te perken, maar om er een nieuwe betekenis aan te geven opdat die niet als dekmantel zou worden gebruikt om schade aan te richten.

Digitaal geweld is niet onvermijdelijk; er bestaan oplossingen. Sommige daarvan gaan over verbeterde moderatie, transparantie van algoritmes, media-educatie, steun voor slachtoffers en internationale samenwerking. Andere, meer fundamentele oplossingen betreffen de responsabilisering van gebruikers via de invoering van een vertrouwelijk traceerbaarheidssysteem, zoals de door een betrouwbare derde partij geverifieerde pseudonimiteit. Die technische en juridische denkoefening kan evenwel pas echt beginnen als men eerst de omvang en de ernst van de huidige straffeloosheid erkent.

Dat is het doel van dit deel van de toelichting bij dit voorstel: bevestigen dat online geweld een omvangrijk maatschappelijk fenomeen is, een zorgwekkende politieke realiteit en een dringende kwestie die juridische oplossingen vereist. Zolang de samenleving dat geweld tolereert als onvermijdelijk omgevingsruis, zolang ze de slachtoffers in de steek laat, zolang ze weigert haar wetten aan te passen aan de digitale ruimte, draagt ze bij aan de verankering van die straffeloosheid.

Er moet een democratisch debat komen op basis van feiten, dat ruimte biedt aan de ervaring van slachtoffers, modellen vergelijkt en opties beoordeelt. Men kan zich echter niet langer tevredenstellen met algemene beloften. In een democratie is immers niets gevaarlijker dan het idee dat eender welke ruimte een wetteloos gebied kan worden. Vandaag is de digitale ruimte voor een aanzienlijk deel van de bevolking precies zo'n gebied.

De wetgever mag niet langer wegkijken. De geloofwaardigheid van de wet, de bescherming van burgers en het respect dat iedereen mag verwachten van onze instellingen staan op het spel.

4. ***Een einde aan de anonimiteit maar niet aan de privacy***

Een einde maken aan absolute anonimiteit betekent niet dat het recht op privacy wordt afgeschaft. Integendeel, de evolutie naar meer verantwoordelijkheid van de digitale spelers moet worden uitgedacht met strikte inachtneming van dat grondrecht. De uitdaging is groot, maar politiek en technisch haalbaar. Het is niet de bedoeling twee vrijheden tegen elkaar uit te spelen maar ze op elkaar af te stemmen: het beschermde recht op vrije meningsuiting enerzijds en het recht op veiligheid, waardigheid en gerechtigheid anderzijds. De sleutel ligt

légitime. Il ne s'agit pas de brider la liberté d'expression mais de lui redonner du sens en garantissant qu'elle ne soit pas utilisée comme un paravent pour nuire.

Cette violence numérique n'est pas inéluctable; des solutions existent. Certaines concernent la modération renforcée, la transparence algorithmique, l'éducation aux médias, le soutien aux victimes, la coopération internationale. D'autres, plus fondamentales, concernent la responsabilisation des usagers, par la mise en place d'un système de traçabilité confidentielle, comme le pseudonymat vérifié par un tiers de confiance. Mais cette réflexion technique et juridique ne pourra s'ouvrir sérieusement que si l'on reconnaît d'abord l'ampleur et la gravité de l'impunité qui règne actuellement.

C'est l'objectif de cette partie du présent exposé; affirmer que la violence en ligne est un fait social majeur, une réalité politique préoccupante et une urgence appelant des solutions au niveau juridique. Tant que la société tolérera cette violence comme un bruit de fond inévitable, tant qu'elle laissera les victimes seules, tant qu'elle refusera d'adapter son droit à l'espace numérique, elle participera à l'ancrage de cette impunité.

Un débat démocratique doit s'ouvrir. Il doit partir des faits, écouter les victimes, confronter les modèles, évaluer les options. Mais il ne peut plus se contenter de promesses générales. Car dans une démocratie, rien n'est plus dangereux que l'idée qu'un espace, quel qu'il soit, puisse devenir un territoire sans loi. Or, aujourd'hui, pour une partie importante de la population, le numérique est précisément ce territoire.

Il appartient au législateur de sortir de ce déni. Il en va de la crédibilité du droit, de la protection des citoyens et du respect que chacun est en droit d'attendre de nos institutions.

4. ***Mettre fin à l'anonymat sans mettre fin à la vie privée***

Mettre fin à l'anonymat absolu ne signifie pas abolir le droit à la vie privée. C'est, au contraire, dans le respect scrupuleux de ce droit fondamental que doit être pensée toute évolution vers une plus grande responsabilité des acteurs du numérique. Le défi est de taille mais il est politiquement et techniquement surmontable. Il ne s'agit pas d'opposer deux libertés mais de les articuler; le droit à l'expression libre et protégé, d'une part, et le droit à la sécurité, à la dignité, à la justice, également, d'autre part. La clé réside dans un modèle intermédiaire, structuré,

in een gestructureerd en geloofwaardig tussenmodel, namelijk dat van pseudonimiteit in combinatie met een systeem van identiteitscontrole door een betrouwbare derde partij.

Een van de grootste misverstanden in het debat over digitale anonimiteit is de verwarring tussen anonimiteit en vertrouwelijkheid. Absolute anonimiteit, zoals die vandaag bestaat op de meeste digitale platformen, houdt in dat iemand die illegale content plaatst of illegaal gedrag vertoont, lange tijd onbekend kan blijven, ook voor de bevoegde instanties, behalve in uitzonderlijke gevallen die een langdurige gerechtelijke procedure vereisen. Dat systeem werkt straffeloosheid in de hand, zoals hierboven uitgelegd. Vertrouwelijkheid – in de betekenis van bescherming van persoonsgegevens – kan daarentegen worden gevrijwaard in een systeem waarin de gebruiker veilig kan worden geïdentificeerd door een betrouwbare partij, zonder dat de identiteit openbaar wordt gemaakt of wordt gebruikt door privébedrijven.

In een dergelijk model van gecontroleerde pseudonimiteit kunnen gebruikers een zichtbaar pseudoniem (gebruikersnaam, nickname, avatar) blijven gebruiken, terwijl hun echte identiteit indien nodig in situaties die onder wettelijke regels vallen, via een bevoegde derde instantie toegankelijk wordt gemaakt. Die derde partij kan een openbare instantie zijn (een overheidsinstantie, regulator of onafhankelijke instantie) of een privéactor, op voorwaarde dat die is erkend, aan strikte regels is onderworpen en regelmatig wordt gecontroleerd. Die derde partij staat niet in voor controle, maar moet te allen tijde de traceerbaarheid van de gebruiker garanderen, onder precieze en proportionele wettelijke voorwaarden.

Dat systeem wordt impliciet al toegepast bij veel gevoelige digitale procedures. Wanneer een Belgische burger online een bankcontract ondertekent, een belastingaangifte doet of toegang krijgt tot een medische dienst, wordt zijn identiteit gecontroleerd via gecertificeerde digitale middelen (zoals de Itsme-app, de eID-kaart of andere door de overheid erkende toepassingen). De dienstverlener beschikt niet noodzakelijk over die gegevens; hij weet alleen dat de gebruiker door een erkende betrouwbare derde partij is geauthenticeerd. Dat mechanisme kan worden doorgetrokken naar de sociale media, mits het toepassingsgebied, de garanties en de technische voorwaarden ervan worden afgebakend.

Identificatie voorafgaand aan het openen van een account op een platform betekent niet dat de gebruiker zijn identiteit aan het publiek of aan het bedrijf zelf moet bekendmaken. Het volstaat dat het verificatiesysteem op de achtergrond certificeert dat achter de account daadwerkelijk een echte persoon zit, identificeerbaar door de bevoegde instanties.

crédible; celui du pseudonymat adossé à un système de vérification d'identité par un tiers de confiance.

L'un des principaux malentendus entourant le débat sur l'anonymat numérique tient à une confusion entre anonymat et confidentialité. L'anonymat absolu, tel qu'il existe aujourd'hui sur la majorité des plateformes numériques, signifie que l'auteur d'un contenu ou d'un comportement illicite peut rester durablement inconnu, y compris des autorités compétentes, sauf dans des cas exceptionnels nécessitant une procédure judiciaire lourde. Ce régime favorise l'impunité, comme cela a été exposé précédemment. À l'inverse, la confidentialité, au sens de la protection des données personnelles, peut tout à fait être préservée dans un système où l'utilisateur est identifiable de manière sécurisée par un acteur de confiance, sans que cette identité soit exposée au public, ni exploitée par des entreprises privées.

Ce modèle de pseudonymat vérifié permet aux utilisateurs de continuer à utiliser un pseudonyme visible (nom d'usage, alias, avatar) tout en rendant leur identité réelle accessible, en cas de nécessité dans des situations visées par des règles légales, via une tierce entité habilitée. Cette tierce entité peut être publique (comme un organe de l'État, un régulateur, une autorité indépendante) ou privée, à condition qu'elle soit agréée, soumise à un encadrement strict et auditée de manière régulière. Son rôle n'est pas de surveiller mais de garantir, à tout moment, la traçabilité potentielle de l'utilisateur, dans des conditions légales précises et proportionnées.

Ce système est déjà d'application, de manière implicite, dans de nombreuses démarches numériques sensibles. Lorsqu'un citoyen belge signe un contrat bancaire en ligne, effectue une déclaration d'impôts ou accède à un service médical, son identité est vérifiée via des moyens numériques certifiés (tels que l'application Itsme, la carte eID ou d'autres applications reconnues par les autorités). L'opérateur du service ne détient pas nécessairement ces données; il sait seulement que l'utilisateur a été authentifié par un tiers de confiance agréé. Ce mécanisme peut être transposé aux réseaux sociaux, à condition d'en définir le périmètre, les garanties, et les modalités techniques.

L'identification préalable à l'ouverture d'un compte sur une plateforme n'implique pas que l'utilisateur doive révéler son identité au public ou à l'entreprise elle-même. Il suffit que le système de vérification certifie, en arrière-plan, qu'un individu réel, identifiable par les autorités compétentes, est bien à l'origine de ce compte.

Met dat principe, toegepast op de digitale wereld, zou de vrijheid van meningsuiting onder een pseudoniem kunnen worden gegarandeerd, veralgemeende controle worden voorkomen en misstanden drastisch worden teruggedrongen. Er zou ruimte voor expressie zijn waarbij iedereen weet dat zijn acties uiteindelijk traceerbaar zijn in geval van een ernstige overtreding van de wet, zonder dat daarom zijn identiteit blijvend of onterecht wordt bekendgemaakt.

Die aanpak is gebaseerd op een aantal essentiële beschermingsmaatregelen. Ten eerste kan de toegang tot de werkelijke identiteit enkel worden verleend door de gerechtelijke autoriteiten, in het kader van een procedure die in overeenstemming is met het Belgische recht. Ten tweede zouden de platformen zelf geen identiteitsgegevens bewaren. Ze zouden enkel verplicht zijn om bij de aanmaak van een account te interageren met de betrouwbare derde partij. Ten derde moeten de controlemechanismen voldoen aan hoge veiligheidscriteria, interoperabel, voor iedereen toegankelijk en aan kwetsbare doelgroepen aangepast zijn.

Er moet bijzondere aandacht gaan naar het risico op overdreven gegevenscentralisatie. Om elk bigbrothereffect te voorkomen, is het essentieel dat de gekozen oplossing gebaseerd is op een gedecentraliseerd en pluralistisch model, in overeenstemming met de AVG. Veeleer dan met één monopolistische speler zou kunnen worden gewerkt met een register van erkende actoren, die allemaal aan dezelfde eisen inzake transparantie, veiligheid en democratische controle moeten voldoen. Het gaat om een logica van een gereguleerd ecosysteem, niet om een toezichtstructuur.

In België is aan alle voorwaarden voldaan om een dergelijke architectuur op te zetten. Er bestaat een juridisch raamwerk voor digitale identificatie, de technische expertise is beschikbaar en de tools worden dagelijks door miljoenen burgers gebruikt. Het enige wat ontbreekt, is politieke actie opdat die technische capaciteit door de overheid zou worden benut. Het is niet de bedoeling een nieuw toezichtsysteem op te zetten, maar een vangnet te creëren om de verantwoordelijkheden te kunnen identificeren in een omgeving waar momenteel elke transparantie zoek is.

Een terugkerend bezwaar tegen dit model is de noodzakelijke anonimiteit voor klokkenluiders, dissidenten in autoritaire regimes of mensen die in hun nabije omgeving worden bedreigd. Het is essentieel uitzonderingen te behouden om die mensen te beschermen, alsook echt anonieme kanalen in stand te houden waarlangs men zijn mening kan uiten, wanneer het algemeen belang of de veiligheid van mensen dergelijke kanalen rechtvaardigen. Die uitzonderingen moeten strikt, doelgericht

Appliqué au numérique, ce principe permettrait de préserver la liberté d'expression sous pseudonyme, d'éviter la surveillance généralisée et de réduire drastiquement les abus. Il créerait un espace d'expression où chacun sait que ses actes sont, *in fine*, traçables en cas de manquement grave à la loi, sans que cela implique une exposition permanente ou injustifiée de son identité.

Cette approche repose sur une série de garde-fous essentiels. Premièrement, l'accès à l'identité réelle ne pourrait être opéré que par les autorités judiciaires, dans le cadre d'une procédure conforme au droit belge. Deuxièmement, aucune donnée d'identité ne serait conservée par les plateformes elles-mêmes; elles seraient seulement tenues d'interagir avec le tiers de confiance au moment de la création du compte. Troisièmement, les mécanismes de vérification devraient répondre à des critères de sécurité élevés, être interopérables, accessibles à tous, et adaptés aux publics vulnérables.

Une attention particulière doit être portée au risque de centralisation excessive des données. Pour éviter tout effet "Big Brother", il est fondamental que la solution adoptée repose sur un modèle décentralisé et pluraliste, en conformité avec le RGPD. Plutôt qu'un seul acteur monopolistique, il peut exister un registre d'acteurs agréés, tous soumis aux mêmes exigences de transparence, de sécurité et de contrôle démocratique. La logique est celle d'un écosystème régulé et non d'une structure de surveillance.

En Belgique, les conditions sont réunies pour mettre en place une telle architecture. Le cadre juridique de l'identification numérique existe, l'expertise technique est disponible, les outils sont utilisés quotidiennement par des millions de citoyens. Il ne manque qu'un acte politique pour que cette capacité technique soit exploitée par l'autorité publique. Il ne s'agit pas de construire un nouveau système de surveillance mais d'instituer un filet de sécurité permettant d'identifier les responsabilités là où règne aujourd'hui l'opacité.

Une objection récurrente à ce modèle est celle de la nécessité de l'anonymat pour les lanceurs d'alerte, les dissidents dans des régimes autoritaires, ou les personnes menacées dans leur environnement proche. Il est essentiel de maintenir des exceptions visant la protection de ces personnes et des canaux d'expression réellement anonymes dans les cas où l'intérêt général ou la sécurité des personnes le justifie. Ces exceptions doivent être définies de manière stricte, ciblée et encadrée. Elles ne

en met de nodige voorwaarden worden gedefinieerd. In democratische samenlevingen met een solide rechtsstaat kunnen ze geen rechtvaardiging vormen voor het behoud van een absolute en veralgemeende anonimiteit voor iedereen.

In werkelijkheid vormt niet de afschaffing van de anonimiteit een probleem, maar het ongedifferentieerde gebruik ervan, waardoor de bedreigde journalist, de stalker van jongeren, de betaalde politieke internettrol en de gewone internetgebruiker over één kam worden geschoren. Het is de verantwoordelijkheid van de wetgever om onderscheid te maken tussen situaties, een beschermingshiërarchie op te stellen en ervoor te zorgen dat de beginselen van gerechtigheid niet wijken voor technisch gemak of moreel relativisme.

Geverifieerde pseudonimiteit vormt absoluut geen aanslag op de persoonlijke levenssfeer, maar kan die juist versterken. Ze maakt het mogelijk machtsmisbruik, identiteitsfraude en desinformatiecampagnes te beperken, zonder dat de gewone gebruikers de controle over hun persoonlijke gegevens verliezen. Ze herstelt de mogelijkheid om in normale omstandigheden in rechte op te treden, zijn rechten te doen gelden en te leven in een veilige digitale ruimte.

Er zij aan herinnerd dat de bescherming van de persoonlijke levenssfeer niet betekent dat wordt gewaarborgd dat openbaar gedrag totaal ondoorzichtig is, maar inhoudt dat wordt voorkomen dat een dergelijk gedrag ongerechtvaardigde, ongeoorloofde of onrechtmatige commerciële vormen aanneemt. In een democratie is de persoonlijke levenssfeer verenigbaar met verantwoordelijkheid; belangrijk is dat de identificatiemechanismen proportioneel, gerechtvaardigd, gecontroleerd en omkeerbaar zijn. Dat is net het doel van het systeem dat via dit voorstel van resolutie wordt beoogd.

Het zou verkeerd zijn te denken dat dit model technisch onhaalbaar is. Meerdere proefprojecten in andere domeinen hebben aangetoond dat identiteitsverificatiemechanismen haalbaar zijn zonder overdreven gegevensverzameling. Er zijn internationale standaarden aan het ontstaan, gebaseerd op de principes van *privacy by design*, dus op een architectuur waar de vertrouwelijkheid al in het ontwerp van het systeem is geïntegreerd. Het is dan ook perfect mogelijk een Belgische of zelfs Europese oplossing uit te werken die deze principes in acht neemt en tegelijk een einde maakt aan de veralgemeende onverantwoordelijkheid.

Het moet geen abrupte breuk zijn, maar een weloverwogen overgang naar een gezonde regulering van de digitale wereld, gestoeld op transparantie, subsidiariteit en de eerbiediging van de grondrechten.

sauraient justifier le maintien d'un anonymat absolu et généralisé pour tous, dans des sociétés démocratiques disposant d'un État de droit solide.

Dans les faits, ce n'est pas la suppression de l'anonymat qui poserait problème mais son usage indistinct, qui mettrait sur le même plan le journaliste menacé, le harceleur d'adolescents, le troll politique rémunéré et l'internaute lambda. La responsabilité du législateur est de distinguer les situations, de hiérarchiser les protections et de garantir que les principes de justice ne cèdent pas devant la facilité technique ou le relativisme moral.

Le pseudonymat vérifié, loin d'être une atteinte à la vie privée, peut au contraire la renforcer. Il permet de limiter les abus de pouvoir, les usurpations d'identité, les campagnes de désinformation, sans pour autant exposer les utilisateurs ordinaires à une perte de contrôle sur leurs données personnelles. Il rétablit la possibilité d'agir en justice dans des conditions normales, de faire respecter ses droits, de vivre dans un espace numérique sécurisé.

Il faut rappeler que la protection de la vie privée ne consiste pas à garantir l'opacité totale des comportements publics mais à éviter qu'ils prennent des formes injustifiées, commerciales illicites ou abusives. Dans une démocratie, la vie privée est compatible avec la responsabilité; ce qui importe, c'est que les mécanismes d'identification soient proportionnés, justifiés, encadrés et réversibles. C'est précisément l'objectif du système que la présente proposition de résolution vise à instaurer.

Il serait faux de croire que ce modèle est techniquement irréalisable. Plusieurs expériences pilotes, dans d'autres domaines, ont montré la faisabilité de mécanismes de vérification d'identité sans collecte excessive de données. Des standards internationaux émergent, basés sur des principes de *privacy by design*, c'est-à-dire sur une architecture où la confidentialité est intégrée dès la conception du système. Il est donc parfaitement possible de créer une solution belge, voire européenne, qui respecte ces principes tout en mettant fin à l'irresponsabilité généralisée.

Loin d'être une rupture brutale, il doit s'agir d'une transition mesurée vers une régulation saine du numérique, fondée sur la transparence, la subsidiarité et le respect des droits fondamentaux.

België kan en moet een leidende rol spelen in die ontwikkeling; ons land kan opwerpen dat het einde van de anonimiteit niet het einde van de vrijheid betekent en een stap is naar een gedeelde en beschermde burgerlijke vrijheid.

In een wereld waarin de publieke opinie vandaag grotendeels online wordt gevormd, is de verantwoordelijkheid van de digitale spelers een democratische vereiste. De oplossing zal niet van de platformen of de techreuzen komen, maar wel van de staten die hun reguleringsplicht durven op te nemen zonder toe te geven aan de verleiding om op te geven of autoritarisme vrij spel te geven. België kan een van die staten zijn.

5. ***Gedaan met afwachten, tijd voor digitaal leiderschap***

Op het gebied van digitale regelgeving balanceren de Europese staten te vaak tussen institutionele verlamming en een reflex tot overmatig delegeren. Verlamming wanneer de omvang van de uitdaging of de technische complexiteit voorwendsels worden om niets te ondernemen. Overmatig delegeren wanneer de politieke verantwoordelijkheid wordt overgelaten aan de platformen zelf of niet wordt genomen onder het voorwendsel dat er supranationale normen zullen komen, die evenwel eeuwig op zich laten wachten. Door die dubbele valstrik wordt slechts traag vooruitgang geboekt, nemen de wantoestanden toe en erodeert het respect voor de fundamentele beginselen. In het licht van die realiteit moet België een duidelijke keuze maken; het kan niet langer een afwachtende houding aannemen, maar moet daarentegen een voortrekkersrol op zich nemen in het opbouwen van een verantwoordelijke digitale wereld.

Het idee dat een legitiem antwoord alleen uit Europese hoek kan komen, kan geen reden zijn om niets te doen. Uiteraard is een geharmoniseerde regelgeving in de hele Europese Unie wenselijk en zelfs noodzakelijk om te zorgen voor een efficiënte, samenhangende en niet-gefragmenteerde digitale markt. De Europese Unie kan er echter slechts op vooruitgaan indien een aantal van haar lidstaten bereid is concrete oplossingen te verkennen, voor te stellen en te testen. Door op nationaal niveau aan te tonen dat een model levensvatbaar, evenwichtig en evenredig is, kunnen de voorwaarden worden gecreëerd voor uitbreiding naar het Europese niveau.

België is van oudsher een drijvende kracht in tal van domeinen die verband houden met de burgerlijke vrijheden, de regulering van nieuwe technologieën en digitale ethiek. Het beschikt thans over de nodige infrastructuur, instellingen, expertise en rechtsinstrumenten om opnieuw een laboratorium te worden voor experimenten om de actoren van de digitale wereld verantwoordelijkheidszin

La Belgique peut et doit jouer un rôle moteur dans cette évolution; elle peut affirmer que la fin de l'anonymat ne signifie pas la fin de la liberté et constitue un pas vers une liberté civique partagée et protégée.

Dans un monde où l'opinion publique se façonne désormais largement en ligne, la responsabilité des acteurs du numérique est une exigence démocratique. La solution ne viendra pas des plateformes, ni des grandes puissances technologiques. Elle viendra des États qui osent assumer leur devoir de régulation, sans céder à la tentation de l'abandon ou de l'autoritarisme. La Belgique peut être l'un de ces États.

5. ***Refuser l'attentisme en assumant un leadership numérique***

Dans le champ de la régulation numérique, les États européens oscillent trop souvent entre la paralysie institutionnelle et le réflexe de déléguer à outrance. Paralysie, lorsque l'ampleur du défi ou la complexité technique deviennent des prétextes à l'inaction. Délégation à outrance lorsque la responsabilité politique est abandonnée aux plateformes elles-mêmes ou non assumée sous le prétexte que des normes supranationales vont exister mais dont la concrétisation s'éternise. À cause de ce double piège, les avancées tardent, les dérives s'aggravent et le respect des principes fondamentaux s'effrite. Face à cette réalité, la Belgique doit faire un choix clair; refuser l'attentisme et assumer un rôle de précurseur dans la construction d'un monde numérique responsable.

L'idée selon laquelle seule une réponse européenne serait légitime à ces enjeux ne peut, à elle seule, justifier l'immobilisme. Bien sûr, une régulation harmonisée à l'échelle de l'Union européenne est souhaitable, nécessaire même, pour garantir l'efficacité, la cohérence et la non-fragmentation du marché numérique. Mais l'Union européenne ne peut avancer que si certains de ses États membres acceptent d'explorer, de proposer, de tester des solutions concrètes. C'est en démontrant, au niveau national, qu'un modèle est viable, équilibré, proportionné, que l'on crée les conditions de son élargissement au niveau européen.

La Belgique a historiquement joué ce rôle d'aiguillon dans plusieurs domaines liés aux libertés publiques, à la régulation des nouvelles technologies ou à l'éthique numérique. Elle dispose aujourd'hui des infrastructures, des institutions, des expertises et des instruments juridiques nécessaires pour redevenir un laboratoire pour les expériences permettant de responsabiliser les acteurs du

bij te brengen en die wereld aldus democratischer te maken. Het kan een paradigmaverschuiving teweegbrengen die innovatie, vrijheid en regulering met elkaar verzoent, en een geloofwaardig tegenmodel bieden voor commerciële deregulering of autoritair toezicht.

Op nationaal vlak bestaan alvast hefbomen voor actie. België beschikt over een robuust kader voor digitale identificatie, via wijdverbreide tools zoals Itsme of de elektronische identiteitskaart. Die middelen maken het mogelijk de identiteit van een burger op een veilige, vertrouwelijke en bij wet afdwingbare wijze te verifiëren zonder de persoonsgegevens aan derden bloot te stellen. Technisch zou het mogelijk zijn deze tools (of andere vergelijkbare oplossingen) aan te wenden voor het verkrijgen van toegang tot de digitale platformen waarop het risico van desinformatie, belaging of uitbuiting van minderjarigen het grootst is.

Bovendien is het Belgische institutionele landschap bijzonder geschikt voor de implementatie van een ernstig, rechtsconform proefproject. De Gegevensbeschermin gsautoriteit (GBA), de sectorregulatoren, de diensten van de FOD Justitie, de FOD Beleid en Ondersteuning (BOSA) en vele andere competente actoren zouden kunnen bijdragen aan een evenwichtig raamwerk voor een pseudonimiteitssysteem met verificatie door een betrouwbare derde partij.

Die wens om op nationaal niveau op te treden is niet onverenigbaar met een Europese strategie. Integendeel, verenigbaarheid is een voorwaarde voor geloofwaardigheid. Als België wil wegen op de toekomstige gesprekken over de evolutie van de *Digital Services Act*, de plaats van digitale identificatie in de toekomstige regelgeving over artificiële intelligentie of initiatieven om online geweld te bestrijden, moet het kunnen bogen op concrete ervaring, op een *corpus* van duidelijke voorstellen, op een legitimiteit vanuit concrete oplossingen die tot voorbeeld kunnen strekken.

Recente belangrijke Europese normen zijn aldus tot stand gekomen: door de actieve inzet van lidstaten die het voortouw namen en bij machte bleken praktische oplossingen aan te dragen zonder te verzanden in al te technische debatten of verlamd te geraken door een slappe consensus. Frankrijk heeft een voorstrekkersrol gespeeld in de regulering van haatdragende inhoud, Duitsland in algoritmische transparantie en Ierland in de samenwerking met de platformen. België kan op zijn beurt een leidende rol spelen in de link tussen individuele verantwoordelijkheid en digitale traceerbaarheid.

Dat vereist een duidelijke en vaste politieke wil, ondersteund door een coherente diplomatieke strategie.

monde numérique et, ainsi, de le rendre démocratique. Elle peut amorcer un changement de paradigme qui réconcilie l'innovation, la liberté et la régulation et offrir un contre-modèle crédible à la dérégulation commerciale ou à la surveillance autoritaire.

Sur le plan national, plusieurs leviers d'action sont d'ores et déjà disponibles. La Belgique dispose d'un cadre robuste en matière d'identification numérique, via des outils largement adoptés comme l'application Itsme ou la carte d'identité électronique. Ces dispositifs permettent de vérifier l'identité d'un citoyen de manière sécurisée, confidentielle et juridiquement opposable, sans exposer ses données personnelles à des tiers. Il serait techniquement possible d'envisager leur usage (ou celui de solutions analogues) dans le cadre de l'accès aux plateformes numériques les plus exposées à la désinformation, au harcèlement ou à l'exploitation des mineurs.

En outre, le paysage institutionnel belge est particulièrement adapté à la mise en œuvre d'un projet pilote sérieux, respectueux du droit. L'autorité pour la protection des données (APD), les régulateurs sectoriels, les services du SPF Justice, du SPF Stratégie & Appui (BOSA) et bien d'autres sont autant d'acteurs compétents qui pourraient contribuer à la définition d'un cadre équilibré pour la mise en œuvre d'un système de pseudonymat vérifié par un tiers de confiance.

Cette volonté d'agir au niveau national n'est pas incompatible avec une stratégie européenne. Au contraire, elle en constitue la condition de crédibilité. Si la Belgique veut peser dans les discussions à venir sur l'évolution du *Digital Services Act*, sur la place de l'identification numérique dans le futur règlement sur l'intelligence artificielle ou sur les initiatives de lutte contre les violences en ligne, elle doit pouvoir s'appuyer sur une expérience concrète, sur un *corpus* de propositions claires, sur une légitimité acquise par des solutions concrètes pouvant servir d'exemple.

C'est ainsi que se sont imposées les grandes normes européennes récentes; à partir de la mobilisation d'États membres jouant un rôle moteur, capables d'apporter des solutions de terrain afin de ne pas s'éterniser dans des débats trop souvent technicisés ou paralysés par le consensus mou. La France a ouvert la voie sur la régulation des contenus haineux, l'Allemagne sur la transparence algorithmique, l'Irlande sur la coopération avec les plateformes; la Belgique peut, à son tour, jouer ce rôle moteur sur la question du lien entre la responsabilité individuelle et la traçabilité numérique.

Cela suppose une volonté politique claire, assumée et articulée à une stratégie diplomatique cohérente. Il

Het doel is niet eenzijdig een norm op te leggen of te handelen buiten het Europese kader om, maar een legitiem initiatief te nemen in het licht van de ernst van de zaak, de dringende noodzaak om minderjarigen te beschermen, de omvang van online geweld en de groeiende behoefte van de burgers aan een rechtvaardige en doeltreffende regelgeving.

Die leiderspositie zou des te meer gerechtvaardigd zijn daar België momenteel een centrale rol speelt in een aantal grote digitale uitdagingen. Als hoofdstad van de Europese Unie en thuishaven van tal van multilaterale instellingen, niet-gouvernementele organisaties en technische en politieke denktanks heeft België een internationale uitstraling die het in staat stelt om het vraagstuk diplomatiek, academisch en regelgevend aan de orde te stellen. In dat opzicht zou beleidsverzuim meer zijn dan een vergissing; het zou een verloochening zijn van de legitieme invloed die ons land zou kunnen uitoefenen.

Tot slot is dat leiderschap niet alleen strategisch of diplomatiek, maar ook moreel. De Belgische Staat moet bevestigen dat hij weigert de huidige straffeloosheid in de digitale ruimte als onontkoombaar te beschouwen, online geweld te normaliseren, of de coherentie van de rechtsstaat op te offeren wegens de vermeende technische complexiteit van de digitale ruimte. Een dergelijk leiderschap draait niet om toezicht of repressie, maar komt voort uit een democratisch model waarin de betrokken spelers verantwoordelijkheid nemen in de digitale ruimte, net zoals ze dat doen in de fysieke ruimte.

De digitale ruimte mag niet langer een vrijplaats van onverantwoordelijkheid zijn. Het is tijd om in die ruimte genuanceerd maar standvastig de principes toe te passen waarop ons sociaal contract is gebaseerd. Dat vereist moed, rechtlijnigheid en het vermogen om uit de patronen van eindeloze terughoudendheid te stappen. België heeft daarvoor de middelen. Het moet nu ook de wil hebben om tot actie over te gaan.

6. ***De Kamer van volksvertegenwoordigers, dé plaats voor dit democratische debat***

De digitalisering werkt fundamenteel in op ons democratisch bestel. Sociale relaties worden anders ingevuld, de manier waarop mensen zich uitdrukken verandert, de symbolische macht wordt herschikt en miljoenen burgers krijgen te maken met nieuwe risico's. De evolutie is zodanig groot dat niets doen geen optie is. Evenmin mag overhaast te werk worden gegaan. Allereerst is er nood aan een duidelijk, gestructureerd, onderbouwd en doorgedreven parlementair debat.

ne s'agit pas d'imposer unilatéralement une norme, ni d'agir en dehors du cadre européen mais de prendre une initiative légitime au regard de la gravité des enjeux, de l'urgence à protéger les mineurs, de l'ampleur des violences en ligne et de l'attente croissante des citoyens d'une régulation juste et efficace.

Cette position de leadership serait d'autant plus justifiée que la Belgique est aujourd'hui au cœur d'une série d'enjeux numériques majeurs. Capitale de l'Union européenne, siège de nombreuses institutions multilatérales et d'organisations non gouvernementales, de plateformes de réflexion sur les plans technique et politique, elle dispose d'un rayonnement international qui lui permettrait de porter cette question sur la scène diplomatique, académique et réglementaire. À ce titre, refuser d'agir serait plus qu'une erreur; ce serait une renonciation à l'influence que notre pays pourrait légitimement exercer.

Enfin, le leadership dont il est ici question n'est pas seulement stratégique ou diplomatique; il est moral. Il s'agit pour l'État belge d'affirmer qu'il refuse de considérer comme inéluctable l'impunité régnant dans le numérique, qu'il refuse de normaliser la violence en ligne, qu'il refuse de sacrifier la cohérence de l'État de droit à cause de la prétendue complexité technique du monde numérique. Ce leadership n'est pas celui de la surveillance ni de la répression, c'est celui d'un modèle démocratique où les acteurs concernés assument et prennent leurs responsabilités dans l'espace numérique comme il les assument dans l'espace physique.

Le numérique ne peut plus être le continent de l'irresponsabilité. Il est temps d'y appliquer, avec nuance mais fermeté, les principes qui fondent notre contrat social. Cela suppose du courage, de la rigueur et une capacité à sortir des schémas d'attente perpétuelle. La Belgique en a les moyens. Elle doit désormais en avoir la volonté.

6. ***La Chambre des représentants, lieu de ce débat démocratique***

Le numérique transforme profondément les fondements de notre vie démocratique. Il restructure les relations sociales, modifie les modalités d'expression, redistribue les pouvoirs symboliques et expose des millions de citoyens à des risques nouveaux. Face à l'ampleur de ces mutations, la première pire réponse serait le silence et la deuxième pire réponse serait la précipitation. Ce qu'il faut, à ce stade, c'est un débat parlementaire clair, structuré, informé, exigeant.

Dat debat moet plaatsvinden waar de democratie wordt uitgedacht, bediscussieerd en vormgegeven: in de Kamer van volksvertegenwoordigers. Niet om knopen definitief door te hakken en stante pede een oplossing te vinden, en nog minder om in allerijl wetgeving te maken, maar om een politiek kader te bieden voor een noodzakelijk debat, dat terecht op gang is gebracht door de federale regering en met name de minister van Modernisering van de overheid, belast met Overheidsbedrijven, Ambtenarenzaken, het Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid.

De minister voor Digitalisering heeft in meerdere recente openbare verklaringen aangegeven dat ze de discussie wil openen over het opheffen van internetanonimiteit en over de leeftijdscontrole voor toegang tot sociale media. Zij stelde voor die discussie eerst in het parlementaire kader te voeren voordat eventueel een wetsontwerp aan de Kamer van volksvertegenwoordigers wordt voorgelegd. Die aanpak valt toe te juichen, aangezien ze het evenwicht tussen de machten respecteert, de rol van de wetgevende macht benadrukt en ruimte schept om dit complexe, heikele onderwerp op een transparante en pluralistische manier te bespreken.

Dit voorstel van resolutie dient dan ook vanuit die optiek te worden gelezen. Het is niet de bedoeling een unieke technische oplossing voor te schrijven, noch dat de Kamer van volksvertegenwoordigers de rol van de regering overneemt. De bedoeling is een formeel debat op gang te brengen, de kwestie van de verantwoordelijkheid van de digitale spelers op de politieke agenda te zetten en de institutionele voorwaarden te scheppen voor een collectieve beraadslaging op basis van onderbouwde, weloverwogen en gedeelde standpunten.

Bij die beraadslaging moeten niet alleen actoren op het terrein (leerkrachten, magistraten, slachtoffers, platformen, regulatoren, technische deskundigen, verenigingen voor de bescherming van rechten) worden gehoord, maar ook nagedacht over de fundamentele beginselen die we in de digitale ruimte wensen te verdedigen. Hoe kunnen de vrijheid van meningsuiting, de bescherming van de minderjarigen, de privacy en de individuele verantwoordelijkheid met elkaar worden verzoend? Welke beschermingsmaatregelen zijn nodig om misstanden te voorkomen? Met welke technische architectuur kan de traceerbaarheid worden gegarandeerd zonder overdreven controle? In welke wettelijke uitzonderingen moet worden voorzien en hoe kunnen die worden geflankeerd?

De Kamer van volksvertegenwoordigers moet die vragen niet zelf beantwoorden, maar ervoor zorgen dat er uitgebreid over kan worden nagedacht, zonder zinloze polemieken en ideologische stellingnames. Met

Ce débat doit se tenir là où la démocratie se pense, se confronte, se construit; au sein de la Chambre des représentants. Non pas pour trancher définitivement une question et trouver immédiatement une solution, encore moins pour légiférer dans l'urgence mais pour donner un cadre politique à une réflexion nécessaire, engagée à bon droit par le gouvernement fédéral et en particulier par la ministre de l'Action et de la Modernisation publiques, chargée des Entreprises publiques, de la Fonction publique, de la Gestion immobilière de l'État, du Numérique et de la Politique scientifique.

Dans plusieurs interventions publiques récentes, la ministre du numérique a exprimé sa volonté d'ouvrir la discussion sur la fin de l'anonymat en ligne et sur la vérification de l'âge pour l'accès aux réseaux sociaux. Elle a proposé que cette discussion s'engage d'abord dans le cadre parlementaire avant qu'un éventuel projet de loi ne soit soumis à la Chambre des représentants. Cette démarche est à saluer; elle respecte l'équilibre des pouvoirs, valorise le rôle du pouvoir législatif et permet un traitement transparent et pluraliste d'un sujet aussi complexe que sensible.

C'est dans cette perspective que s'inscrit la présente proposition de résolution. Elle n'entend pas prescrire une solution technique unique, ni substituer le rôle de la Chambre des représentants à celui du gouvernement. Elle vise à formaliser l'ouverture d'un débat, à inscrire la question de la responsabilité des acteurs du numérique à l'agenda politique et à créer les conditions institutionnelles d'une délibération collective, sur des bases documentées, argumentées et partagées.

Cette délibération doit non seulement permettre d'auditionner les acteurs de terrain (enseignants, magistrats, victimes, plateformes, régulateurs, experts techniques, associations de protection des droits) mais aussi de s'interroger sur les principes fondamentaux que nous voulons défendre dans l'espace numérique. Comment articuler la liberté d'expression, la protection des mineurs, la vie privée et la responsabilité individuelle? Quels garde-fous pour éviter les abus? Quelle architecture technique pour garantir la traçabilité sans surveillance excessive? Quelles exceptions légitimes et comment les encadrer?

Le rôle de la Chambre des représentants n'est pas de répondre seule à ces questions mais de garantir qu'elles soient posées avec sérieux, en dehors des polémiques éphémères et des postures idéologiques.

het huidige gebrek aan transparantie, de heersende onmacht en de technische achterpoortjes worden immers noch de slachtoffers, noch de vrijheden beschermd. De heersende status quo houdt de illusie van neutraliteit in stand, maar bestendigt in werkelijkheid een door de platformen gedomineerd bedrijfsmodel, ten koste van het algemeen belang.

Door dit debat te openen, zou de Kamer van volksvertegenwoordigers erkennen dat de verantwoordelijkheid van de digitale spelers een democratische uitdaging van het hoogste belang is. De Kamer zou haar rol opnemen als forum voor bemiddeling tussen expertise, politieke gevoeligheden en verwachtingen van de burgers. Ze zou vorm geven aan een uitgebalanceerde regulering, gebaseerd op recht, rede en de wens dat de digitale wereld niet langer een vrijplaats is zonder gemeenschappelijke regels.

Op basis daarvan zou de regering vervolgens een wetsontwerp kunnen opstellen, onderbouwd door parlementaire discussies, hoorzittingen en de verzamelde expertise. De regering zou dan een beslissing met kennis van zaken kunnen nemen en een technisch haalbare en juridisch onderbouwde oplossing kunnen voorstellen, dat aan het Belgische model is aangepast en andere Europese landen tot voorbeeld kan strekken.

Dit voorstel van resolutie beoogt geenszins beperkingen op te leggen. Het kondigt ook niet voortijdig een hervorming aan. Het behelst een democratische methode in drie fasen: debat, hoorzitting en uitwerking. Het voorstel van resolutie komt tegemoet aan de oproep van de bevoegde minister. Het zorgt ervoor dat de Kamer van volksvertegenwoordigers haar rol kan opnemen op een gebied dat tot nu toe al te vaak werd overgelaten aan het oordeel van platformen of regelgevende instanties bevoegd voor technische aspecten.

In een tijd waarin wantrouwen jegens instellingen vaak ontstaat door de indruk dat de beslissende debatten elders worden gevoerd, heeft dit initiatief ook een sterke symbolische betekenis. Met dit voorstel wordt bevestigd dat de regulering van de digitale wereld onder de soevereiniteit van de democratische staat valt en dat die soevereiniteit hier in het Parlement, op methodische, strikte en verantwoordelijke wijze wordt uitgeoefend.

Car le *statu quo* actuel (fait d'opacité, d'impuissance, de contournements techniques) ne protège ni les victimes, ni les libertés. Il entretient une illusion de neutralité alors qu'il consacre en réalité un modèle commercial dominé par les plateformes, au détriment de l'intérêt général.

En ouvrant ce débat, la Chambre des représentants reconnaîtrait que la responsabilité des acteurs du numérique est un enjeu démocratique de premier ordre. Elle assumerait son rôle d'espace de médiation entre les expertises, les sensibilités politiques et les attentes citoyennes. Elle donnerait corps à une régulation équilibrée, fondée sur le droit, la raison et la volonté que le numérique ne soit plus un territoire d'exception sans application des règles communes.

Le gouvernement, sur cette base, pourrait ensuite élaborer un projet de loi, nourri par les échanges parlementaires, les auditions, les expertises rassemblées. Il pourrait arbitrer en connaissance de cause, proposer une solution techniquement viable et juridiquement fondée, adaptée au modèle belge et potentiellement inspirante au niveau européen.

La présente proposition de résolution ne vise pas à imposer la moindre contrainte. Elle n'annonce pas prématurément une réforme. Elle propose une méthode démocratique en trois phases: débattre, écouter et construire. Elle répond à l'invitation de la ministre compétente. Elle permet à la Chambre des représentants d'assumer son rôle dans un sujet qui, jusqu'ici, a trop souvent été laissé à la seule appréciation des plateformes ou des organes régulateurs compétents dans les domaines techniques.

À une époque où la défiance envers les institutions est souvent alimentée par l'impression que les débats décisifs se jouent ailleurs, cette démarche a aussi une portée symbolique forte. Elle affirme que la régulation du numérique relève de la souveraineté de l'État démocratique et que cette souveraineté s'exerce ici, dans l'enceinte parlementaire, avec méthode, avec rigueur, avec responsabilité.

Ismaël Nuino (Les Engagés)

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. gelet op Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaledienstenverordening), meer bepaald op artikel 28 ervan aangaande de online bescherming van minderjarigen;

B. gelet op Verordening (EU) 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG;

C. gelet op Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);

D. gelet op Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit;

E. overwegende dat onvoorwaardelijke online anonimiteit een gevoel van straffeloosheid in de hand werkt dat een voedingsbodem creëert voor geweld, haat, belaging of manipulatie, waardoor het openbare debat vervuild geraakt;

F. overwegende dat de grote digitale platformen thans zonder enig democratisch mandaat de publieke ruimte grotendeels vormgeven, volgens commerciële logica's die moeilijk te verzoenen vallen met de eerbied voor de menselijke waardigheid en de grondrechten;

G. overwegende dat de huidige, vaak geautomatiseerde moderatiesystemen veruit ontoereikend zijn om een afdoend antwoord te bieden op online geweld, desinformatie en de wildgroei van probleemaccounts;

H. overwegende dat het massale gebruik van sociale media door minderjarigen, soms van kinds af, vaak plaatsvindt zonder enige vorm van gedegen leeftijdscontrole, aangezien de huidige veiligheidssystemen louter pro forma en dus omzeilbaar zijn;

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. vu le Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) et notamment son article 28 concernant la protection des mineurs en ligne;

B. vu le Règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE;

C. vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données);

D. vu le Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique;

E. considérant que l'anonymat absolu en ligne favorise un sentiment d'impunité, qui alimente des comportements violents, haineux, harcelants ou manipulateurs, contribuant à la détérioration du débat public;

F. considérant que les grandes plateformes numériques structurent désormais une grande partie de l'espace public, sans mandat démocratique, selon des logiques commerciales peu compatibles avec la protection de la dignité humaine et des droits fondamentaux;

G. considérant que les mécanismes actuels de modération, souvent automatisés, sont largement insuffisants pour répondre efficacement aux violences en ligne, à la désinformation et à la prolifération de comptes problématiques;

H. considérant que l'accès massif des mineurs aux réseaux sociaux, parfois dès l'enfance, se fait souvent en dehors de tout contrôle réel de l'âge, les barrières actuelles étant purement déclaratives et donc contournables;

I. overwegende dat het gebrek aan leeftijdsverificatie minderjarigen blootstelt aan onaangepaste inhoud, kwaadwillige verzoeken en potentieel destructieve sociale dynamieken, met name cyberpesten;

J. overwegende dat het structurele onvermogen om de daders van onwettig online gedrag snel en zeker te identificeren de gerechtelijke respons uitholt, de slachtoffers verhindert hun rechten uit te oefenen en een algemeen klimaat van onverantwoordelijkheid voedt;

K. overwegende dat de invoering van een systeem van geverifieerde pseudonimiteit via een betrouwbare onafhankelijke derde het mogelijk zou maken daders van onwettige handelingen te identificeren zonder het recht op privacy van de gewone gebruikers op de helling te zetten;

L. overwegende dat dat model kan worden gebouwd op reeds bestaande technische infrastructuur, alsook een rechtsgrond en gedegen waarborgen zou bieden inzake veiligheid en gegevensbescherming;

M. overwegende dat de minister van Modernisering van de overheid, belast met Overheidsbedrijven, Ambtenarenzaken, het Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid, openlijk de wens heeft uitgesproken om een parlementair debat te houden over dit vraagstuk;

VERZOEKT DE FEDERALE REGERING:

1. op basis van het parlementaire debat en van de aanbevelingen die voortkomen uit de hoorzittingen in de Kamer van volksvertegenwoordigers, een wetsontwerp uit te werken tot invoering van een systeem van geverifieerde pseudonimiteit van gebruikers van digitale platformen, waarbij zowel de juridische traceerbaarheid van accounts als de doeltreffende bescherming van de privacy van de gebruikers worden gewaarborgd;

2. op basis van het parlementaire debat en van de aanbevelingen die voortkomen uit de hoorzittingen in de Kamer van volksvertegenwoordigers, met name voor minderjarigen een betrouwbaar en beveiligd leeftijdsverificatiesysteem in te stellen voor toegang tot sociale media of andere gevoelige platformen, dat werkt met een betrouwbare derde en ervoor zorgt dat de desbetreffende platformen zelf geen gevoelige gegevens kunnen verzamelen;

3. op Europees niveau een initiatief te nemen om die vereisten op het gebied van identificatie en bescherming van minderjarigen te harmoniseren, teneinde omzeiling

I. considérant que l'absence de vérification d'âge expose les mineurs à des contenus inadaptés, à des sollicitations malveillantes et à des dynamiques sociales potentiellement destructrices, notamment le cyberharcèlement;

J. considérant que l'incapacité structurelle à identifier rapidement et sûrement les auteurs de comportements illégaux en ligne affaiblit la réponse judiciaire, empêche les victimes d'exercer leurs droits et alimente un climat général d'irresponsabilité;

K. considérant que la mise en place d'un système de pseudonymat vérifié, reposant sur un tiers de confiance indépendant, permettrait d'identifier des auteurs d'actes illicites sans remettre en cause le droit à la vie privée des utilisateurs ordinaires;

L. considérant que ce modèle pourrait s'appuyer sur des infrastructures techniques déjà existantes et offrirait un encadrement juridique et des garanties élevées en matière de sécurité et de protection des données;

M. considérant que la ministre de l'Action et de la Modernisation publiques, chargée des Entreprises publiques, de la Fonction publique, de la Gestion immobilière de l'État, du Numérique et de la Politique scientifique, a exprimé publiquement le souhait qu'un débat parlementaire soit organisé sur cette question;

DEMANDE AU GOUVERNEMENT:

1. d'élaborer, sur la base du débat parlementaire et des recommandations élaborées suite aux auditions au sein de la Chambre des représentants, un projet de loi instaurant un mécanisme de pseudonymat vérifié pour les utilisateurs de plateformes numériques, garantissant à la fois la traçabilité judiciaire des comptes et la protection effective de la vie privée des utilisateurs;

2. de mettre en place, sur la base du débat parlementaire et des recommandations élaborées suite aux auditions au sein de la Chambre des représentants, un système fiable et sécurisé de vérification de l'âge pour l'accès aux réseaux sociaux, ou à d'autres plateformes sensibles notamment pour les mineurs, en s'appuyant sur un tiers de confiance et en évitant la collecte de données sensibles par les plateformes elles-mêmes;

3. de porter au niveau européen une initiative visant à harmoniser ces exigences en matière d'identification et de protection des mineurs afin d'éviter les contournements

te voorkomen en een samenhangend regelgevend kader uit te bouwen voor de digitale wereld.

14 juni 2025

et d'assurer une cohérence réglementaire dans l'espace numérique.

14 juin 2025

Ismaël Nuino (Les Engagés)

Centrale drukkerij - Imprimerie centrale