DOC 56 **0725/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

17 februari 2025

WETSVOORSTEL

teneinde de burgerlijke rechtspleging open te stellen voor slachtoffers van vermeend onwettige, anoniem verrichte internetactiviteiten, en artikel XII.20 van het Wetboek van economisch recht te wijzigen

(ingediend door de heer Khalil Aouasti c.s.)

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

17 février 2025

PROPOSITION DE LOI

ouvrant la voie civile aux victimes d'activités supposées illicites exercées de manière anonyme sur Internet et modifiant l'article XII.20 du Code de droit économique

(déposée par M. Khalil Aouasti et consorts)

SAMENVATTING

Dit wetsvoorstel heeft hoofdzakelijk tot doel cyberpesten tegen te gaan door de voorzitter van de rechtbank van eerste aanleg de mogelijkheid te bieden de verantwoordelijken van digitale platforms te verplichten tot mededeling van alle informatie waarover zij beschikken en die nuttig is voor het onderzoek naar en het vaststellen van de inbreuken die door derden via hun platforms werden gepleegd, meer bepaald met het oog op de identificatie van die derden. Aldus moet worden gewaarborgd dat de slachtoffers van cyberpesters snel en doeltreffend worden beschermd. Tegelijk is het de bedoeling dat de cyberpesters tegen ontradende sancties kunnen aanlopen.

RÉSUMÉ

La présente proposition de loi vise, en substance, à lutter contre le cyberharcèlement en permettant au président du tribunal de première instance d'ordonner aux responsables des plateformes numériques de communiquer toutes les informations dont ils disposent et qui sont utiles à la recherche et à la constatation d'infractions commises par des tiers par leur intermédiaire, en vue notamment d'identifier ces tiers. La finalité est de garantir une protection rapide et efficace aux victimes des cyberharceleurs et d'assurer que des sanctions dissuasives puissent les frapper.

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*

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,

Dit voorstel neemt met een aantal aanpassingen de tekst over van voorstel DOC 55 3971/001.

1. **Inleidende beschouwingen**

Cyberpesten is een probleem dat de hele samenleving treft. Het uit zich in spot, belediging, haatdragende of vernederende uitlatingen enzovoort en richt zich vooral tegen jongeren, studenten en journalisten. Niemand blijft van dergelijke wandaden gevrijwaard, maar het weze opgemerkt dat cyberpesters het veelal op vrouwen gemunt hebben.

Iedereen weet dat cyberpesten het leven van een slachtoffer kan verwoesten. Daarom moeten alle mogelijkheden – ook op juridisch vlak – worden aangewend om het slachtoffer te beschermen en de cyberpester te straffen.

Laatstgenoemde verschuilt zich vaak achter anonimiteit of een pseudoniem. Het feit dat men geen verhaal heeft tegen de dader die verantwoordelijk is voor dergelijke dreigementen, beledigingen, intimidaties enzovoort brengt bij het slachtoffer bijkomend leed teweeg. Om die redenen wil de indiener van dit wetsvoorstel dat de platforms meer bijdragen aan een snelle identificatie van cyberpesters. Zonder actieve medewerking van de platforms krijgen de laffe individuen die zich achter een pseudoniem verschuilen een gevoel van straffeloosheid.

De platforms kunnen de onwettige inhoud op verzoek van de slachtoffers weliswaar verwijderen, maar dat neemt niet weg dat die slachtoffers niet over een burgerrechtelijke mogelijkheid beschikken om de daders die dergelijke zaken vanuit een georganiseerde anonimiteit publiceren, te doen vervolgen.

Niemand is veilig voor denigrerende en beledigende campagnes op sociale media. Nadat in België meerdere mediafiguren het slachtoffer zijn geworden van cyberpesten, hebben de RTBF en de VRT de overheid opgeroepen tot actie. De RTBF, de VRT, de Franstalige en Nederlandstalige verenigingen van journalisten, alsook de Association des journalistes professionnels (AJP) en de Vlaamse Vereniging van Journalisten (VVJ), hebben een gezamenlijke oproep tot een wetgevend initiatief gedaan. Die oproep vindt zijn weerklank in dit wetsvoorstel, dat beoogt dat de plegers van het voormelde digitaal geweld daadwerkelijk burgerrechtelijk kunnen worden vervolgd.

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

La présente proposition reprend, en l'adaptant le texte de la propositions DOC 55 3971/001.

1. **Considérations introductives**

Le cyberharcèlement est un fléau qui touche l'ensemble de la société. Ce fléau peut prendre la forme de moqueries, d'insultes, de propos haineux, humiliants, etc.. Il peut toucher en particulier les jeunes, les étudiants et les journalistes. Personne n'est à l'abri de ces actes de malveillance et il faut noter que, souvent, les femmes sont davantage visées par les cyberharceleurs.

On sait que le cyberharcèlement peut détruire la vie d'une victime. Et nous devons nous doter de tous les instruments – notamment juridiques – qui permettent à la fois de protéger la victime et de sanctionner le cyberharceleur.

Le cyberharceleur se cache souvent derrière l'anonymat ou un pseudonyme. Quant à la victime, la circonstance de ne pas être en mesure de se retourner contre l'auteur responsable de ces menaces, insultes, intimidations, etc., représente une souffrance supplémentaire. Pour ces raisons, nous souhaitons vraiment faire davantage contribuer les plateformes afin d'identifier rapidement les cyberharceleurs. Sans une collaboration active des plateformes, ces individus lâches se réfugiant derrière un pseudonyme ont un sentiment d'impunité.

Si les plateformes, à la demande des victimes, retirent les publications illicites, il n'en demeure pas moins que les victimes ne peuvent pas ensuite poursuivre les auteurs de telles publications qui se cachent derrière l'anonymat organisé sur le plan civil.

Personne n'est à l'abri de campagnes de dénigrements et d'insultes diffusées sur les réseaux sociaux. À la suite du cyberharcèlement frappant plusieurs personnalités médiatiques dans notre pays, la RTBF et la VRT ont demandé aux autorités de réagir. La RTBF, la VRT, les associations de journalistes francophones et néerlandophones ainsi que l'Association des journalistes professionnels (AJP) et la Vlaamse Vereniging van Journalisten (VVJ), se sont réunies afin d'encourager une initiative législative que nous proposons de reprendre pour permettre la poursuite civile effective contre les auteurs de telles violences numériques.

Cyberpesten[1] is een kwaal die steeds meer mensen in de samenleving treft. Uit recent Frans onderzoek blijkt dat 20 % van de adolescenten en 60 % van de jongeren tussen 18 en 25 jaar slachtoffer is geweest van cyberpesten.[2] Wanneer dat pesten anoniem of onder pseudoniem gebeurt, is dat des te harder voor de slachtoffers en is het ook moeilijk om het te stoppen.

Dit wetsvoorstel wil een mogelijkheid tot gerechtelijke actie bieden aan de slachtoffers van vermeend onwettige inhoud (bijvoorbeeld bedreigende, belagende, lasterlijke, onterende, kwetsende, haatdragende, racistische, xenofobe, negationistische of revisionistische content) die anoniem of onder pseudoniem op het internet en op sociale media wordt verspreid[3] en die een ernstige aantasting van hun rechten vormt. Het is de bedoeling dat die slachtoffers via de burgerlijke rechtspleging een zaak kunnen aanspannen tegen cyberpesters die zulke content verspreiden, teneinde herstel te verkrijgen voor de geleden schade, wat thans niet mogelijk is.

2. **Wanneer vermeend onwettige inhoud anoniem of onder een pseudoniem wordt verspreid, zijn de door de digitale platforms aangereikte oplossingen ontoereikend**

Wanneer op internet en op sociale media vermeend onwettige inhoud wordt verspreid die de rechten van een persoon ernstig aantast, kan het slachtoffer van die inhoud contact opnemen met de platforms (Facebook, X (voorheen Twitter), Instagram of TikTok bijvoorbeeld) waarop de inhoud werd geplaatst. De door de platforms voorgestelde oplossingen houden echter alleen in dat – zo het de platforms belieft – dergelijke inhoud wordt verwijderd en/of het profiel van de daders wordt opgeschort dan wel verwijderd, zonder dat het de daders voorts wordt verboden nieuwe profielen aan te maken.

In de praktijk leidt de melding nooit tot de identificatie van de auteurs van de vermeend onwettige inhoud, terwijl die identificatie de slachtoffers net in de mogelijkheid zou stellen om voor de rechtbank een vergoeding te eisen voor de geleden schade.

1 Cyberpesten kan vele vormen aannemen, zoals intimidatie, beledigingen, spot of bedreigingen, het verspreiden van geruchten, het hacken van accounts en diefstal van een digitale identiteit, het op sociale media aanmaken van een discussietopic, een groep of een pagina met de bedoeling iemand op de korrel te nemen, het plaatsen van foto's of video's van iemand in een minder flatterende houding enzovoort.

2 *https://www.rtbf.be/article/plus-d-un-ieune-sur-deux-a-deia-ete-victime-de-cyber-harcelement-11.100.695 (8 november 2022)*

3 Ongeacht of zulks schriftelijk dan wel via geluidsfragmenten, niet-bewegende beelden of video's geschiedt.

Le cyberharcèlement[1] est l'un des maux qui frappent un nombre grandissant de personnes dans notre société. Une récente étude française a démontré que 20 % des adolescents et 60 % des 18-25 ans ont été victimes de cyberharcèlement[2]. Lorsqu'ils sont anonymes ou effectués sous couvert de pseudonymes, les actes de cyberharcèlement sont particulièrement difficiles à vivre pour leurs victimes et il est compliqué d'y mettre un terme.

La présente proposition de loi a pour but de donner aux victimes de contenus supposés illicites, diffusés[3] de manière anonyme ou par voie de pseudonymes sur Internet et sur les réseaux sociaux, – tels que les contenus menaçants, harcelants, calomnieux, diffamatoires, injurieux, haineux, racistes, xénophobes, négationnistes ou révisionnistes –, et portant gravement atteinte à leurs droits, la possibilité d'agir en justice contre les auteurs de tels contenus, par la voie civile, pour obtenir réparation du dommage qu'elles ont subi, ce qui n'est actuellement pas possible.

2. **En cas de contenus supposés illicites diffusés anonymement ou sous couvert de pseudonymes, les solutions proposées par les plateformes numériques sont insuffisantes**

En cas de diffusion, sur Internet et sur les réseaux sociaux, de contenus supposés illicites portant gravement atteinte aux droits d'une personne, la victime de ces contenus peut s'adresser aux plateformes telles que Facebook, X (anciennement Twitter), Instagram ou TikTok, sur lesquelles ces contenus ont été publiés. Mais les solutions proposées par les plateformes permettent uniquement – selon le bon vouloir de ces dernières – d'obtenir la suppression de ces contenus et/ou la suspension ou la suppression du profil de leurs auteurs, sans qu'il ne soit par ailleurs interdit à ces derniers de créer de nouveaux profils.

Le signalement effectué n'aboutit en pratique jamais à une identification des auteurs des contenus supposés illicites, alors même que cette identification permettrait aux victimes de solliciter, en justice, la réparation du dommage qu'elles ont subi.

1 Les actes de cyberharcèlement peuvent prendre plusieurs formes, telles que les intimidations, insultes, moqueries ou les menaces en ligne, propagations de rumeurs, piratages de comptes et usurpations d'identité digitale, les créations d'un sujet de discussion, d'un groupe ou d'une page sur un réseau social à l'encontre d'une personne, les publications de photos ou vidéos d'une personne en mauvaise posture, etc.

2 *https://www.rtbf.be/article/plus-d-un-ieune-sur-deux-a-deia-ete-victime-de-cyber-harcelement-11.100.695 (8 novembre 2022)*

3 Que ce soit par écrits, sons, images fixes ou vidéos.

Overeenkomstig artikel XII.20, § 1, eerste lid, van het Wetboek van economisch recht (hierna “het WER”), hebben de intermediaire dienstverleners (waaronder de sociale media) “geen algemene verplichting om toe te zien op de informatie die zij doorgeven of opslaan, noch om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden.”

Een bijzondere of specifieke verplichting tot toezicht werd evenwel ingesteld. Artikel XII.20, § 2, eerste lid, van het WER bepaalt immers dat de intermediaire dienstverleners tot medewerking zijn gehouden, daar zij verplicht zijn “de bevoegde gerechtelijke of administratieve autoriteiten onverwijld in kennis te stellen van vermeende onwettige activiteiten of onwettige informatie die door de afnemers van hun dienst worden geleverd.”

De dienstverlener kan zelf invulling geven aan die medewerking dan wel tussenbeide komen op verzoek van de gerechtelijke autoriteiten.

Zo de dienstverlener medewerking weigert, kan hij worden bestraft met een sanctie van niveau 3 (strafrechtelijke geldboete van 26 tot 25.000 euro, vermeerderd met de opdeciemen).

In de praktijk wordt die sanctie nooit toegepast en voor zover bekend werden de platforms, niettegenstaande tal van weigeringen tot medewerking, nog nooit aansprakelijk gesteld. Vastgesteld wordt dat wanneer een platform weigert de auteur van vermoedelijk onwettige inhoud te identificeren, het gerechtelijk onderzoek of het opsporingsonderzoek afgesloten wordt en de zaak geseponeerd wordt.

De door de platforms voorgestelde oplossingen zijn duidelijk ontoereikend, zozeer zelfs dat het slachtoffer van vermeend onwettige inhoud ertoe wordt gedwongen in rechte op te treden.

3. **Er kunnen geen civielrechtelijke stappen worden ondernomen tegen iemand die anoniem of onder een pseudoniem vermeend onwettige inhoud verspreidt**

De civielrechtelijke procedures zijn helaas onbruikbaar.

De burgerlijke rechter kan immers aan iedere gedingvoerende partij wel bevelen het bewijsmateriaal dat zij bezit, over te leggen, overeenkomstig artikel 871 van het Gerechtelijk Wetboek, en de burgerlijke rechter kan in

Conformément à l’article XII. 20, § 1er, alinéa 1er, du Code de droit économique (ci-après CDE), les prestataires intermédiaires, en ce compris les réseaux sociaux, “n’ont aucune obligation générale de surveiller les informations qu’ils transmettent ou stockent, ni aucune obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites.”

Toutefois, une obligation particulière ou spécifique de surveillance a été mise en place. L’article XII. 20, § 2, alinéa 1er, du CDE exige des prestataires intermédiaires qu’ils collaborent avec les autorités judiciaires ou administratives compétentes dès lors qu’ils sont informés de l’existence d’“activités illicites alléguées qu’exerceraient les destinataires de leurs services, ou d’informations illicites alléguées que ces derniers fourniraient.”

Cette “collaboration” peut être le fait du prestataire ou intervenir “à la demande des autorités judiciaires”.

En cas de refus de collaboration, le prestataire est passible d’une sanction de niveau 3 (amende pénale de 26 à 25.000 euros majorée des décimes additionnels).

Dans les faits, cette sanction n’est jamais appliquée et la responsabilité des plateformes n’a, à notre connaissance, encore jamais été mise en cause nonobstant de nombreux refus de collaboration. L’on constate en pratique que, lorsque l’identification de l’auteur d’un contenu supposé illicite est refusée par une plateforme, l’instruction ou l’information judiciaire se clôture par un classement sans suite.

Les solutions proposées par les plateformes sont de toute évidence insuffisantes, à telle enseigne que la victime de contenus supposés illicites est alors contrainte d’agir en justice.

3. **La voie civile est impossible contre un auteur anonyme de contenus supposés illicites ou ayant recours à un pseudonyme pour diffuser ces contenus**

La voie judiciaire civile est toutefois impraticable.

En effet, si le juge civil peut ordonner à toute partie litigante de produire les éléments de preuve dont elle dispose, conformément à l’article 871 du Code judiciaire, et si le juge civil peut aussi ordonner, en vertu de

het raam van een hangend geschil derden ook bevelen stukken te bezorgen, overeenkomstig artikel 877 van hetzelfde Wetboek[4], maar de onderzoekshandelingen die door de burgerlijke rechter kunnen worden bevolen om het bewijs van feiten te leveren, vereisen dat de partijen tegen wie vorderingen worden ingesteld, eerst worden geïdentificeerd en bij de zaak worden geroepen. Zulks veronderstelt dat de civielrechtelijke procedure al is ingeleid.

Op basis van de huidige wettelijke grondslag kunnen de slachtoffers van door anonieme personen verspreide vermeend onwettige inhoud niet verkrijgen dat de anonieme auteur van die content wordt geïdentificeerd. Bijgevolg kunnen zij geen burgerlijke aansprakelijkheidsvordering instellen.

Wanneer de auteur van vermeend onwettige inhoud niet eerst wordt geïdentificeerd, is het dus voor de slachtoffers onmogelijk om hun zaak voor een burgerlijke rechter te brengen teneinde vergoeding voor de geleden schade te verkrijgen.

Die juridische leemte heeft tot gevolg dat de slachtoffers van een mogelijk misdrijf het keuzerecht[5] wordt ontnomen dat zij genieten op grond van artikel 4, eerste lid, van de voorafgaande titel van het Wetboek van Strafvordering, meer bepaald het recht om de zaak aanhangig maken bij de burgerlijke rechtbank dan wel zich burgerlijke partij stellen voor de strafrechtbank (in voorkomend geval na het indienen van een strafklacht).

4. **De strafrechtelijke rechtspleging is praktisch onbruikbaar in geval van schriftelijk cyberpesten, omdat de handelingen in kwestie als een drukpersmisdrijf zouden worden beschouwd**

Het slachtoffer moet dus een strafklacht indienen om de identificatiegegevens van de auteur van vermeend onwettige inhoud te verkrijgen.

Eens de dader geïdentificeerd, is het om tot een proces te kunnen komen nog nodig dat de feiten niet als drukpersmisdrijf worden beschouwd.

Ter herinnering: het drukpersmisdrijf is een misdrijf (misdaad, wanbedrijf of overtreding) dat neerkomt op de uitdrukking van een idee of een mening via de pers

[4] Art. 877 van het Gerechtelijk Wetboek: “Wanneer er ernstige en bepaalde aanwijzingen bestaan dat een partij of een derde een stuk onder zich heeft dat het bewijs inhoudt van een ter zake dienend feit, kan de rechter bevelen dat het stuk of een eensluidend verklaard afschrift ervan bij het dossier van de rechtspleging wordt gevoegd.”

[5] A. Verheylesonne, *La prescription de l'action civile née d'une infraction pénale*, in B. Bovy (dir.), *La prescription en matière pénale*, vijfde uitgave, Brussel, Larcier, 2020, blz. 104.

l’article 877 du même Code[4], dans le cadre d’un litige pendant, à des tiers de produire des documents, les mesures d’instruction susceptibles d’être ordonnées par le juge civil pour établir la preuve de faits, imposent que les parties à l’encontre desquelles des prétentions sont formulées soient préalablement identifiées et appelées à la cause. Ceci suppose que le procès civil est déjà introduit.

Les victimes de contenus illicites anonymes ne peuvent obtenir, au regard des fondements légaux actuels, l’identification de l’auteur d’un contenu supposé illicite. Ce qui fait obstacle à leur action en responsabilité civile.

À défaut d’identification préalable de l’auteur d’un contenu supposé illicite, il est donc impossible, pour les victimes, de saisir un juge civil afin d’obtenir la réparation de leur préjudice.

Ce vide juridique a pour effet d’ôter aux victimes d’un potentiel délit, le droit d’option[5] qui leur est conféré par l’article 4, alinéa 1er, du titre préliminaire du Code de procédure pénale, consistant, soit à agir devant le juge civil, soit à se constituer partie civile devant le juge pénal (le cas échéant après avoir déposé une plainte au pénal).

4. **La voie pénale est inopérante en cas de cyberharcèlement écrit en ce qu’il constituerait un délit de presse**

La victime est dès lors contrainte de déposer une plainte pénale pour obtenir les données d’identification de l’auteur de contenus supposés illicites.

Lorsque l’auteur a été identifié, encore faut-il, pour qu’un procès se tienne, que les faits ne relèvent pas du délit de presse.

Pour rappel, le délit de presse est une infraction (crime, délit ou contravention), qui renferme l’expression d’une pensée ou d’une opinion, commise par la voie de

[4] Art. 877 du Code judiciaire: “Lorsqu'il existe des indices sérieux et précis de la détention par une partie ou un tiers, d'un document contenant la preuve d'un fait pertinent, le juge peut ordonner que ce document ou une copie de celui-ci certifiée conforme, soit déposé au dossier de la procédure.”

[5] A. Verheylesonne, “La prescription de l'action civile née d'une infraction pénale”, in B. Bovy (dir.), La prescription en matière pénale, Ve éd., Bruxelles, Larcier, 2020, p. 104.

(waartoe ook internet wordt gerekend), met een bepaalde openbaarheid. Het is bekend dat sinds de arresten van het Hof van Cassatie van 6 maart 2012 elke schriftelijke strafbare meningsuiting op internet een drukpersmisdrijf uitmaakt.[6]

Het probleem is dat de drukpersmisdrijven volgens artikel 150 van de Grondwet tot de exclusieve bevoegdheid van het hof van assisen behoren en dat alleen de door racisme ingegeven drukpersmisdrijven onder de bevoegdheid van de correctionele rechtbank vallen.

De "gewone" drukpersmisdrijven worden in België niet langer strafrechtelijk vervolgd, aangezien het parket er blijkbaar aan heeft verzaakt het hof van assisen voor dergelijke zaken te adiëren (op één recente uitzondering[7] na).[8]

Bijgevolg worden via het internet verspreide geschriften (of beelden dan wel video's met schriftelijk commentaar) die haatboodschappen, geweldaansporingen of bedreigingen inhouden, of die beogen de rust van de geviseerde personen ernstig te verstoren, niet berecht en genieten ze een feitelijke straffeloosheid, ten nadele van de slachtoffers.

Concreet wordt het slachtoffer op die manier geconfronteerd met de absurde incoherentie dat het strafrechtelijk actie moet ondernemen om de identificatie van een onwettig profiel te verkrijgen. Als dat profiel wordt geïdentificeerd, blijft het gedekt door het geheim van het gerechtelijk onderzoek of opsporingsonderzoek tot aan het einde van die rechtsplegingsfase en dreigt het te ontsnappen aan elke strafrechtelijke veroordeling, aangezien de bijeenroeping van een hof van assisen te omslachtig, te tijdrovend, te duur enzovoort zou zijn. Bovendien kunnen er tussen het indienen van een klacht en het verkrijgen van dat nutteloze resultaat meerdere jaren verstrijken.

Die procedurele patstelling wordt versterkt door artikel XII.20, § 2, tweede lid, van het WER, dat het volgende bepaalt: "Onverminderd andere wettelijke of reglementaire bepalingen dienen deze dienstverleners [bedoeld in de artikelen XII.17, XII.18 en XII.19] de bevoegde gerechtelijke of administratieve autoriteiten op hun verzoek alle informatie te verschaffen waarover zij beschikken en die nuttig is voor de opsporing en de vaststelling van de inbreuken gepleegd door hun tussenkomst."

6 Cass. 6 maart 2012, AR nr. P.11.0855.N en P.11.1374.N.

7 Zie hof van assisen te Luik, 13 oktober 2021: *https://www.rtbf.be/article/assises-de-lieQe-sami-haenen-condainne-a-12-rnois-avecsursis-pour-delit-de-presse-et-menaces-10.859.414*

8 J. Englebert, *La procédure garante de la liberté d'information*, Anthémis, 2014, blz. 27.

la presse (dont Internet), avec une certaine publicité. On sait que depuis les arrêts de la Cour de cassation du 6 mars 2012[6], toute expression écrite d'une opinion délictueuse quelconque sur Internet est constitutive d'un délit de presse.

L'écueil rencontré est lié au fait que les délits de presse relèvent, selon l'article 150 de la Constitution, de la compétence exclusive de la cour d'assises, seuls les délits de presse inspirés par le racisme relevant de la compétence du tribunal correctionnel.

Les délits de presse "ordinaires" ne sont plus pénalement poursuivis en Belgique dès lors que le parquet semble avoir renoncé (à une exception récente près[7]) à saisir la cour d'assises dans ce domaine.[8]

En conséquence, les écrits (ou les images ou vidéos accompagnées d'écrits) diffusés par le biais d'Internet qui constituent des discours de haine, des incitations à la violence, des menaces ou qui visent à perturber gravement la tranquillité des personnes qu'ils visent, ne sont pas jugés et bénéficient d'une impunité pénale de fait, au préjudice des victimes.

Concrètement, la victime est ainsi confrontée à cette incohérence absurde en ce sens qu'il lui est imposé d'activer la voie pénale pour obtenir l'identification d'un profil litigieux. Profil qui, s'il est identifié, reste couvert par le secret de l'instruction ou de l'information judiciaire jusqu'à l'issue de cette phase procédurale et risque bien d'échapper à toute condamnation pénale, dès lors que la convocation d'une cour d'assises serait trop lourde, trop longue, trop onéreuse, etc.. De surcroît, entre le moment du dépôt d'une plainte et l'obtention de ce résultat inutile, il n'est pas rare que plusieurs années se soient écoulées.

Cette impasse procédurale est renforcée par l'article XII.20, § 2, alinéa 2, du CDE qui prévoit que: "Sans préjudice d'autres dispositions légales ou réglementaires, les mêmes prestataires (c'est-à-dire ceux visés aux articles XII.17, XII.18 et XII.19) sont tenus de communiquer aux autorités judiciaires ou administratives compétentes, à leur demande, toutes les informations dont ils disposent et utiles à la recherche et à la constatation des infractions commises par leur intermédiaire."

6 Cass., 6 mars 2012, RG n° P.11.0855.N et P.11.1374.N.

7 Cour d'assises de Liège, 13 octobre 2021: *https://www.rtbf.be/article/assises-de-lieQe-sami-haenen-condainne-a-12-rnois-avecsursis-pour-delit-de-presse-et-menaces-10.859.414*

8 J. Englebert, "La procédure garante de la liberté d'information", Anthémis, 2014, p. 27.

Die bepaling verleent de mensen die zich het slachtoffer achten van anonieme of via pseudoniemen op het internet verspreide vermeend onwettige inhoud geen subjectief recht om van de bevoegde overheden de informatie te verkrijgen waarmee zij de auteurs van die inhoud burgerrechtelijk kunnen vervolgen.

Het voormelde tweede lid bepaalt immers alleen dat het verschaffen van informatie betrekking heeft op de vaststelling van inbreuken en alleen mogelijk is op verzoek van de autoriteiten, wat elk verzoek vanwege een particulier uitsluit. De betrokken bepaling is dus niet gericht op het vergoeden van het slachtoffer van een onwettige handeling (die bovendien strafrechtelijk gezien niet noodzakelijk een fout is).

Dat is wat het Hof van Cassatie heeft beslist in zijn arrest[9] van 16 juni 2011, waarmee het Hof het arrest van het hof van beroep te Luik van 22 oktober 2009[10] bevestigde.

Die rechtspraak werd recent toegepast door de rechter in kortgeding van de Franstalige rechtbank van eerste aanleg te Brussel in een beschikking van 4 juli 2022[11].

Daaruit vloeit ten eerste voort dat geen enkele bepaling van het Wetboek van economisch recht de intermediaire dienstverleners ertoe verplicht om de persoonsgegevens van hun gebruikers bekend te maken aan derden die daarom zouden verzoeken.

Het tweede gevolg is dat sociale media die weigeren aan de slachtoffers van lasterlijke of beledigende uitlatingen de identificatiegegevens mee te delen van zij die de uitlatingen deden, niet tekortschieten op het vlak van hun verplichting om zich te gedragen als een normaal voorzichtige en zorgvuldige host.

De rechter in kortgeding heeft bovendien in zijn overweging nr. 42 geoordeeld dat de onmogelijkheid om het verzoek in te willigen het resultaat was van een beleidskeuze van de Belgische wetgever en van een afweging tussen verschillende in het geding zijnde belangen en grondrechten, namelijk het recht op de bescherming van het privéleven en de persoonsgegevens, het recht op de vrijheid van meningsuiting, het recht op leven en op

Cette disposition n'octroie pas aux personnes s'estimant victimes de contenus supposés illicites, anonymes ou diffusés par voie de pseudonymes sur le Web, un droit subjectif leur permettant d'obtenir des autorités compétentes les informations leur permettant de poursuivre civilement les auteurs de ceux-ci.

En effet, cet alinéa 2 susmentionné stipule uniquement que la communication vise la constatation d'infractions et ne peut intervenir qu'"à la demande des autorités", excluant de ce fait toute demande émanant de particuliers. La disposition mise en évidence ne poursuit donc pas un objectif indemnitaire au bénéfice de la victime d'un acte illicite (pouvant par ailleurs ne pas être une faute de nature pénale).

C'est ce qu'a décidé la Cour de cassation dans son arrêt du 16 juin 2011[9], confirmant ainsi l'arrêt de la cour d'appel de Liège du 22 octobre 2009[10].

Cette jurisprudence a été récemment appliquée par la juge des référés du tribunal de première instance francophone de Bruxelles dans une ordonnance du 4 juillet 2022[11].

Il en résulte, premièrement, qu'aucune disposition du Code de droit économique n'impose aux prestataires de services intermédiaires de divulguer les données personnelles de leurs utilisateurs à des tiers qui en feraient la demande.

Deuxièmement, le réseau social qui refuse de communiquer aux victimes de propos calomnieux ou diffamatoires, les données d'identification des auteurs de ces propos, ne manque pas à son obligation de se comporter en hébergeur normalement prudent et diligent.

La juge des référés a en outre estimé, dans le cadre de son attendu n° 42, que l'impossibilité de faire droit à la demande était le résultat "d'un choix politique" du législateur belge et d'une mise en balance "entre de multiples intérêts et droits fondamentaux en cause: le droit à la protection de la vie privée et des données personnelles, le droit à la liberté d'expression, le droit à la vie et à la protection de l'intégrité physique, le droit à un procès

9 Cass., 16 juni 2011, RDTI, 2012, blz. 69 en noot H. Jacquemin, *Qui peut obtenir les informations permettant de rechercher et de poursuivre les auteurs d'infractions commises sur les réseaux?*, blz. 74-81.

10 Luik, 22 oktober 2009, RDTI, 2010/38, blz. 112.

11 Voorz. Rb. Brussel (KG), onuitg., *Revue du droit des technologies de l'information*, nr. 91/2023, blz. 41 e.v.

9 Cass., 16 juin 2011, R.D.T.I., 2012, p. 69 et note H. Jacquemin, "Qui peut obtenir les informations permettant de rechercher et de poursuivre les auteurs d'infractions commises sur les réseaux?", pp. 74-81.

10 Liège, 22 octobre 2009, R.D.T.I., 2010/38, p. 112.

11 Civ. Bruxelles, réf., 4 juillet 2022, inédit, Revue du droit des technologies de l'information, n° 91/2023, p. 41 et svtes.

de bescherming van de fysieke integriteit, het recht op een eerlijk proces enzovoort. De rechter stelde dat het hem in zijn hoedanigheid niet toekwam die beleidskeuze te veranderen of te omzeilen.

5. **De noodzaak om, naar het voorbeeld van Nederland en Frankrijk, de burgerlijke rechtspleging open te stellen voor de slachtoffers van vermeend onwettige activiteiten die anoniem op het internet worden uitgeoefend**

De Belgische wetgever heeft die "politieke keuze" gemaakt in 2013, in de wet van 15 december 2013 tot invoeging van Boek XII ("Recht van de elektronische economie") in het WER[12]. Op dat ogenblik was al 12 % van de kinderen het slachtoffer geweest van cyberpesten. Dat percentage bedroeg 25 % in 2018 en is dus op vijf jaar tijd meer dan verdubbeld. Bovendien is uit een in 2020 door de UNESCO en het International Centre for Journalists (ICFJ) uitgevoerd onderzoek gebleken dat 73 % van de ondervraagde vrouwelijke journalisten al te maken had gekregen met onlinegeweld tijdens hun werk.[13] Die cijfers zijn nog gestegen als gevolg van de pandemie.[14] [15]

De afweging die in 2013 werd gemaakt, is nu duidelijk achterhaald. Gezien de dramatische toename van cyberpesten moet dat ernstige probleem opnieuw worden bekeken. Dat zou moeten leiden tot de openstelling van de burgerlijke rechtspleging (waarop alle slachtoffers wettelijk recht moeten krijgen) voor de slachtoffers van vermeend onwettige en anonieme inhoud op het internet, opdat de betrokkenen met het oog op hun aansprakelijkheidsvordering ten gronde de identiteit van de auteurs van de omstreden content kunnen vernemen.

België zou niet het eerste land zijn dat een dergelijk subjectief recht in zijn wettenarsenaal opneemt. Het recht van de Europese Unie is ter zake duidelijk geen hinderpaal.

12 Wet van 15 december 2013 houdende invoeging van Boek XII, Recht van de elektronische economie, in het Wetboek van economisch recht, en houdende invoeging van de definities eigen aan Boek XII en van de rechtshandhavingsbepalingen eigen aan Boek XII, in de Boeken I en XV van het Wetboek van economisch recht.

13 X., *Online violence against women journalists* (*https://unesdoc.unesco.ora/ark:/48.223/pf 0000375136/PDF/375136enq.pdf.multi%20And%20this%20report%20under%20'other %20tvpes%20of%20discrimination'%20https://en.unesco.orq/sites/default/files/the-chillinQ.pdf)*

14 *https://www.lesoir.be/354.334/article/2021-02-10/la-crise-sanitaire-accelerateur-du-cyberharcelement*

15 *https://www.comparitech.com/fr/cvberharcelement-statistiques/*

équitable, etc.". Choix politique qu'il ne lui revenait pas, en tant que juge, de modifier ou de contourner.

5. **Nécessité d'ouvrir la voie civile aux victimes d'activités supposées illicites exercées de manière anonyme sur Internet, comme aux Pays-Bas ou en France**

Ce "choix politique" du législateur belge a été effectué en 2013, par la loi du 15 décembre 2013 portant insertion du Livre XII, "Droit de l'économie électronique "dans le CDE[12], soit à un moment où 12 % des enfants avaient déjà été victimes de cyberharcèlement en Belgique, ce pourcentage étant passé à 25 % en 2018, soit plus du double en 5 ans[13]. De surcroît, une enquête réalisée en 2020 par l'UNESCO et le Centre international des journalistes (ICFJ) a révélé que 73 % des femmes journalistes interrogées avaient subi des violences en ligne dans le cadre de leur travail[14]. Ces chiffres se sont encore aggravés à la suite de la pandémie.[15]

Manifestement, la mise en balance effectuée en 2013 est aujourd'hui dépassée. Partant, il convient d'opérer, au vu de l'accroissement spectaculaire des cas de cyberharcèlement, une nouvelle appréciation de cette grave problématique. Le résultat devrait déboucher sur l'ouverture de la voie civile (à laquelle toutes les victimes auront légalement droit) aux victimes de contenus supposés illicites et anonymes sur Internet, en leur permettant, préalablement à leur action au fond en responsabilité, d'obtenir l'identification des auteurs des contenus litigieux.

La Belgique ne serait pas le premier pays à insérer un tel droit subjectif dans son arsenal. Et le droit de l'Union européenne ne s'y oppose manifestement pas.

12 Loi du 15 décembre 2013 portant insertion du Livre XII, "Droit de l'économie électronique" dans le Code de droit économique, portant insertion des définitions propres au Livre XII et des dispositions d'application de la loi propres au Livre XII, dans les Livres I et XV du Code de droit économique.

13 *https://www.comparitech.com/fr/cvberharcelement-statistiques/*

14 X., Online violence against women journalists: disponible sur le site: *https://unesdoc.unesco.ora/ark:/48.223/pf 0000375136/PDF/375136enq.pdf.multi%20And%20this%20report%20under%20'other %20tvpes%20of%20discrimination'%20https://en.unesco.orq/sites/default/files/the-chillinQ.pdf*

15 *https://www.lesoir.be/354.334/article/2021-02-10/la-crise-sanitaire-accelerateur-du-cyberharcelement*

5.1. ***De juridische situatie in Nederland***

In Nederland heeft de Hoge Raad in een arrest van 25 november 2005 erkend dat het, wegens de noodwendigheden van een burgerlijke vordering tot vergoeding, de kortgedingrechter toegestaan is om bij voorraad de mededeling van de identificatiegegevens van de vermeende dader van een fout te gelasten.[16]

5.2. ***De juridische situatie in Frankrijk***

Frankrijk beschikt over specifieke wetgeving die het mogelijk maakt de auteur van vermeend onwettige verklaringen op het internet te identificeren, namelijk artikel 145 van de Franse *Code de procédure civile,* dat het volgende bepaalt: "*S'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé*."

In Frankrijk is het dus mogelijk zich te wenden tot een kortgedingrechter opdat die een platform zou verplichten de identificatiegegevens van een of meerdere van zijn gebruikers mee te delen.

De Franse Commission nationale consultative des droits de l'homme (hierna "de CNCDH") heeft de doeltreffendheid van die bepaling onderzocht in haar advies van 8 juli 2021 betreffende de bestrijding van onlinehaatspraak[17]. In punt 20 van haar advies is zij van oordeel dat de identificatie van de auteurs van onwettige inhoud uitermate belangrijk is in de strijd tegen onlinehaatspraak. De CNCDH heeft evenwel ook gewag gemaakt van twee grote knelpunten bij de toepassing van die bepaling.

Het eerste probleem bestaat erin dat er meestal meerdere vorderingen (verzoekschrift of kortgeding) moeten worden ingesteld alvorens een volledige identiteit kan worden verkregen waarmee een civielrechtelijke aansprakelijkheidsvordering kan worden opgestart. Sociale media beschikken meestal alleen over e-mailadressen of IP-adressen, waardoor men zich ook moet wenden tot de serviceproviders (eveneens via een verzoekschrift of kortgeding) om de gegevens van de te identificeren auteur te verkrijgen. Voorafgaande identificatie vereist doorgaans dus twee beschikkingen na verzoekschrift. Dergelijke procedures, waarbij meestal Amerikaanse (of Ierse, afhankelijk van het geval) bedrijven voor de rechter moeten worden gedaagd, zijn erg duur voor de slachtoffers.

[16] Hoge Raad, 25 november 2005,1ER 2006, 2, nota JJC Kabel, betreffende een zaak in verband met intellectuele eigendom.

[17] *https://www.legifrance.gouv.fr/jorf/id/JORFARTI000043851104 #JORFARTI000043851104*

5.1. ***La situation juridique aux Pays-Bas***

Aux Pays-Bas, une décision du Hoge Raad a admis, par un arrêt du 25 novembre 2005, que les besoins d'une action civile en réparation autorisaient le juge des référés à ordonner au provisoire la communication de données d'identification relatives à l'auteur présumé d'une faute.[16]

5.2. ***La situation juridique en France***

La France dispose d'une législation spécifique permettant d'identifier l'auteur de propos supposés illicites sur Internet. Il s'agit de l'article 145 du Code de procédure civile qui énonce ce qui suit: "S'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé."

En France, il est donc possible de saisir un juge des référés pour qu'il contraigne une plateforme à communiquer les données d'identification d'un ou de plusieurs de leurs utilisateurs.

La Commission nationale consultative des droits de l'homme (ci-après CNCDH) a examiné l'efficacité de cette disposition dans son avis du 8 juillet 2021 relatif à la lutte contre la haine en ligne[17]. Sous le point 20 de son avis, la CNCDH estime que l'identification des auteurs de contenus illicites est "un enjeu majeur de la lutte contre la haine en ligne". Toutefois la CNCDH a révélé également des difficultés majeures dans la mise en œuvre de cette disposition. Elles sont au nombre de deux.

La première difficulté réside dans le fait que plusieurs actions (sur requête ou en référé) sont généralement nécessaires avant d'obtenir une identité complète permettant d'introduire l'action civile en responsabilité. Les réseaux sociaux disposent généralement uniquement d'une adresse électronique ou d'adresses IP et il faut alors également s'adresser (toujours par requête ou en référé) aux fournisseurs d'accès pour obtenir les données de l'auteur à identifier. L'identification préalable nécessite donc généralement un système de double ordonnance sur requête. Ces procédures, nécessitant généralement d'attraire devant les juridictions des sociétés américaines (ou le cas échéant irlandaises), représentent un coût très important pour les victimes.

[16] Hoge Raad, 25 novembre 2005,1ER 2006, 2, note JJC Kabel, à propos d'une affaire de propriété intellectuelle.

[17] *https://www legifrance gouvfr/jorf/id/JORFARTI000043851104 #JORFARTI000043851104*

De tweede moeilijkheid heeft te maken met het gebrek aan medewerking vanwege sommige platforms, die talloze procedureargumenten opwerpen (territoriale bevoegdheid van de nationale rechter, onderlinge doorverwijzing tussen Ierland en de Verenigde Staten enzovoort), maar die ook de uitvoerbaarheid van de uitspraken betwisten. De noodzaak om de tenuitvoerlegging van uitgesproken beschikkingen af te dwingen is eveneens heel duur en vertraagt de burgerlijke rechtspleging in grote mate.

5.3. ***Het Unierecht***

Het recht van de Europese Unie verplicht de lidstaten weliswaar niet dergelijke wetgeving aan te nemen, maar sluit die mogelijkheid evenmin uit.

Sinds 25 augustus 2023 zijn grote platforms zoals Facebook, Instagram, X, TikTok enzovoort[18] onderworpen aan de digitaledienstenverordening[19], hierna "de DSA" (*digital services act*).

De voormelde verordening reguleert de internetgiganten en legt de platforms een aantal verplichtingen op, waaronder een moderatieverplichting om onwettige inhoud tegen te gaan. Er zullen meldingstools moeten worden aangeboden. De platforms moeten in elke lidstaat een meldpunt oprichten. Die meldpunten moeten samenwerken met betrouwbare *flaggers;* dat zijn door de lidstaten aangewezen referentie-instellingen. Elke lidstaat moet bovendien over een "digitaledienstencoördinator"[20] beschikken, die wordt belast met het toezicht op de toepassing van de DSA.

Al die maatregelen zijn echter hoofdzakelijk gericht op het verwijderen van via het internet verspreide onwettige inhoud en stellen slachtoffers geenszins in staat om de auteur(s) van dergelijke uitlatingen te identificeren.

Op grond van artikel 10 van de DSA kunnen "de bevoegde nationale gerechtelijke of administratieve autoriteiten" de platforms wel bevelen om "specifieke informatie te verstrekken over een of meerdere specifieke afnemers van de dienst".

La deuxième difficulté est liée au manque de coopération de certaines plateformes qui multiplient les arguments de procédure (compétence territoriale du juge national, renvoi entre l'Irlande et les États-Unis, etc.), mais qui contestent également le caractère exécutoire des décisions prononcées. La nécessité de procéder à une exécution forcée des décisions prononcées entraîne également un coût très important et est de nature à ralentir considérablement la tenue du procès civil.

5.3. ***Le droit de l'Union européenne***

Si le droit de l'Union européenne ne contraint pas les États membres à adopter une telle législation, il n'en exclut pas non plus la possibilité.

Depuis le 25 août 2023, 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)[18], ci-après DSA, est entré en vigueur vis-à-vis des grandes plateformes telles que Facebook, Instagram, X, TikTok, etc.[19]

Afin de réguler les géants du Web, le Règlement précité met en place différentes obligations à charge des plateformes dont celle de modérer les contenus illicites. Des outils de signalement devront être proposés. Les plateformes seront tenues de mettre en place un point de contact dans chaque pays. Ces points de contact devront collaborer avec des "signaleurs de confiance", soit des institutions de référence désignées par les États. Chaque État membre disposera également d'un "coordinateur pour les services numériques"[20]. Ce "coordinateur" sera chargé de surveiller l'application du DSA.

Mais toutes ces mesures visent essentiellement à supprimer les contenus illicites diffusés sur Internet et ne permettent aucunement aux victimes d'identifier les ou l'auteur(s) de tels propos.

L'article 10 du Règlement (UE) 2022/2065 précité (DSA) permet toutefois aux "autorités judiciaires et administratives nationales compétentes" de transmettre aux plateformes des injonctions de fournir des informations spécifiques concernant un ou plusieurs utilisateurs des plateformes.

18 Het betreft de "VLOP" (*very large online platforms*) die door de Europese Commissie zijn opgenoemd.

19 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, PbEU, L 277/1.

20 Voor België zal dat het BIPT zijn.

18 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, JOUE, L 277/1.

19 Soit les "Vlop" (*very large online platforms*) qui ont été désignées par la Commission européenne.

20 En Belgique, ce sera l'IBPT.

Zoals in overweging 31 van de DSA wordt verduidelijkt, behelst de verordening daarentegen geen “rechtsgrond voor het uitvaardigen van dergelijke bevelen, en (…) regelt [zij] evenmin het territoriale toepassingsgebied of de grensoverschrijdende handhaving ervan.”

Het staat dus aan België om zulk wettelijk kader te creëren, bijvoorbeeld door de burgerlijke rechter aan te wijzen als een van de gerechtelijke autoriteiten die bevoegd zijn om dergelijke bevelen uit te vaardigen.

Op 12 juli 2023 hebben het Europees Parlement en de Raad een nieuwe verordening[21] aangenomen, op grond waarvan een onderzoeksrechter (en in sommige gevallen een procureur) Europese bevelen tot verstrekking of bewaring van elektronisch bewijsmateriaal kan uitvaardigen. Die verordening treedt in werking op 18 augustus 2026 en voert een gestandaardiseerde procedure in om exclusief met het oog op strafrechtelijke vervolging de identificatie (en zelfs de verkeers- en locatiegegevens) van auteurs van illegale inhoud te verkrijgen.

Die nieuwe mogelijkheden vormen een grote stap voorwaarts voor de wegwerking van de huidige hinderpalen op strafrechtelijk vlak, want tot dusver is de identificatie van een auteur afhankelijk van de goede wil van de platforms. Vanaf 18 augustus 2026 kan een ongerechtvaardigde identificatieweigering door een platform daadwerkelijk aanleiding geven tot sancties.

Die vooruitgang zal echter niets veranderen aan de procedurele impasse die is ontstaan doordat het publiceren van onwettige inhoud in België als drukpersmisdrijf wordt beschouwd (wanneer de geschriften wel laakbaar maar niet racistisch zijn).

Het blijft dus relevant en nuttig om de burgerlijke rechter de bevoegdheid te verlenen om beschikkingen uit te vaardigen met het oog op de identificatie van de auteur van vermeend onwettige uitlatingen.

Verordening 2023/1543 sluit trouwens geenszins uit dat de lidstaten ervoor zorgen dat identificatie via burgerlijke rechtspleging kan worden afgedwongen. Overweging 22 van die verordening bepaalt uitdrukkelijk: “Deze verordening doet geen afbreuk aan de onderzoeksbevoegdheden van autoriteiten in burgerlijke of administratieve procedures, ook wanneer deze procedures tot sancties kunnen leiden.”

[21] Verordening (EU) 2023/1543 van het Europees Parlement en de Raad van 12 juli 2023 betreffende het Europees verstrekkingsbevel en het Europees bewaringsbevel voor elektronisch bewijsmateriaal in strafzaken en de tenuitvoerlegging van vrijheidsstraffen als gevolg van een strafprocedure, PbEU, L 191/118.

Comme le précise le considérant 31 du DSA, le Règlement n’offre toutefois pas “une base juridique pour l’émission de ces injonctions ni ne réglemente leur champ d’application territorial ou leur exécution transfrontière.”

Il appartient donc à la Belgique de créer ce cadre légal en désignant, par exemple, le juge civil comme étant l’une de ces autorités judiciaires compétentes pour prononcer de telles injonctions.

Le 12 juillet 2023, le Parlement et le Conseil européen ont adopté un nouveau Règlement (UE) 2023/1543[21] permettant à un juge d’instruction (et dans certains cas à un procureur) de prononcer des injonctions européennes de production ou de conservation de preuves électroniques. Ce Règlement, qui entrera en vigueur le 18 août 2026, met en place une procédure standardisée permettant d’obtenir l’identification (et même des données de trafic et de localisation) d’auteurs de contenus illicites, et ce uniquement à des fins de poursuites pénales.

Il s’agit d’une réelle avancée par rapport aux écueils rencontrés actuellement sur le plan pénal, l’identification d’un auteur étant liée au bon vouloir des plateformes. Dès le 18 août 2026, le refus d’identification injustifié opposé par une plateforme pourra donner lieu à des sanctions effectives.

Toutefois, cette avancée ne modifiera aucunement l’impasse procédurale liée à la qualification des contenus illicites en délit de presse en Belgique (s’il s’agit d’écrits délictueux non racistes).

Rendre le juge civil compétent en matière d’injonctions visant à identifier l’auteur de propos supposés illicites reste donc pertinent et utile.

Le Règlement 2023/1543 n’exclut par ailleurs aucunement la possibilité, pour les États membres, d’obtenir une identification par la voie civile. Son considérant 22 prévoit expressément que “Le présent règlement est sans préjudice des pouvoirs d’enquête des autorités dans les procédures civiles ou administratives, notamment lorsque ces procédures peuvent entraîner des sanctions.”

[21] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale, JOUE, L 191/118.

6. **De noodzaak om verschillende grondrechten tegen elkaar af te wegen**

6.1. ***De grondrechten van de dader van de vermeend onwettige activiteit***

Allereerst is het noodzakelijk om elk recht op anonimiteit ten gunste van de dader van de vermeend onwettige activiteit uit te sluiten van de grondrechten die kunnen doorwegen. Die anonimiteit, die juridisch gezien niet bestaat, is louter fictief en wordt op geen enkele manier gegarandeerd door de platforms.

Daarentegen moet rekening worden gehouden met het recht op de eerbiediging van de persoonlijke levenssfeer, het recht op vrijheid van meningsuiting en het recht op de bescherming van de persoonsgegevens.

Evenzo mogen de rechten van verdediging (in rechte) van de dader niet worden geschonden. Hoewel laatstgenoemde per definitie niet aanwezig zal zijn wanneer het verzoek om identificatie wordt ingediend, moeten zijn rechten toch gevrijwaard blijven, aangezien naar aanleiding van de ingestelde vordering ten gronde de grondrechten van alle betrokken partijen tegen elkaar zullen worden afgewogen tijdens een debat op tegenspraak.

In dat verband moet worden opgemerkt dat het Belgisch recht[22] slachtoffers van telefonische belaging nu al de mogelijkheid biedt om van de telecomoperatoren via het telefoonnummer van de beller de identificatie te verkrijgen van de anonieme belager, maar noch vooraf, noch achteraf gaat die identificatie gepaard met de waarborgen die worden geboden door een onafhankelijke en onpartijdige rechter.

6.2. ***De grondrechten van het slachtoffer***

Het gaat in dezen uiteraard om het recht op eer en goede naam, maar in voorkomend geval ook om het recht op menselijke waardigheid. Het is ook een zaak van het recht op daadwerkelijke rechtsbescherming, rekening houdend met het recht op keuze (tussen de strafrechtelijke en de civielrechtelijke rechtspleging) en met de op het drukpersmisdrijf van toepassing zijnde proceduregels (cf. *supra*).

[22] Overeenkomstig artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven heeft de ombudsdienst voor telecommunicatie de opdracht om "van elke persoon die beweert het slachtoffer te zijn van kwaadwillig gebruik van een elektronische communicatienetwerk of -dienst, het verzoek onderzoeken om inlichtingen te krijgen over de identiteit en het adres van de gebruikers van elektronische communicatienetwerken of -diensten die deze persoon hebben lastiggevallen, in zoverre die gegevens beschikbaar zijn. De ombudsdienst willigt het verzoek in indien de volgende voorwaarden vervuld zijn: a) de feiten lijken vast te staan; b) het verzoek heeft betrekking op precieze data en uren."

6. **Nécessité de mettre en balance différents droits fondamentaux**

6.1. ***Les droits fondamentaux de l'auteur de l'activité supposée illicite***

Au préalable, il est nécessaire d'exclure des droits fondamentaux pouvant peser dans la balance, un quelconque droit à l'anonymat au bénéfice de l'auteur de l'activité supposée illicite. Cet anonymat, qui n'existe pas sur le plan juridique, résulte d'une fiction et n'est aucunement garanti par les plateformes.

Le droit au respect de la vie privée, le droit à la liberté d'expression et le droit à la protection des données personnelles doivent en revanche être pris en considération.

Il en va de même des droits de la défense (en justice) de l'auteur. Si celui-ci ne sera, par définition, pas présent lors de la demande d'identification, ces droits seront toutefois préservés dès lors que l'action au fond qui sera intentée permettra, dans le cadre d'un débat contradictoire, une mise en balance des droits fondamentaux de chaque partie en présence.

À cet égard, il convient de constater que le droit belge[22] permet d'ores et déjà aux victimes de harcèlement téléphonique d'obtenir, de la part des opérateurs de télécommunications, l'identification de la personne qui les contacte de manière anonyme à partir de son numéro de téléphone, sans que cette identification ne soit entourée (ni au préalable, ni ultérieurement) des garanties qu'offre un juge indépendant et impartial.

6.2. ***Les droits fondamentaux de la victime***

Il s'agit bien évidemment ici du droit à l'honneur et à la réputation mais également, le cas échéant, du droit à la dignité humaine. Le droit à une protection juridictionnelle effective est également en jeu, compte tenu du droit d'option (entre la voie pénale et la voie civile) et des règles procédurales mises en place dans le cadre du délit de presse (voir ci-dessus).

[22] Conformément à l'article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, le service de médiation des télécommunications est investi de la mission d'"examiner la demande de toute personne se prétendant victime d'une utilisation malveillante d'un réseau ou d'un service de communications électroniques visant à obtenir communication de l'identité et de l'adresse des utilisateurs de réseaux ou de services de communications électroniques l'ayant importunée, pour autant que ces données sont disponibles. Le service de médiation accède à la demande si les conditions suivantes sont réunies: a) les faits semblent établis; b) la demande se rapporte à des dates et heures précises."

In dat verband dient te worden opgemerkt dat het Europees Hof voor de Rechten van de Mens in zijn arrest *K.U. v. Finland*[23] van 2 december 2008 heeft geoordeeld dat praktische en daadwerkelijke bescherming van een minderjarige die het voorwerp is geweest van een seksuele getinte advertentie op het internet, ook inhoudt dat Finland de plicht had doeltreffende maatregelen te nemen om de dader te identificeren en te vervolgen.

6.3. ***Streven naar een evenwicht***

Toestaan dat informatie wordt meegedeeld op basis waarvan burgerrechtelijk kan worden opgetreden tegen de dader van vermeend onwettige activiteiten vormt binnen een democratische samenleving een noodzakelijke, gepaste en evenredige beperking om te verzekeren dat de rechten en vrijheden van een ander worden geëerbiedigd.

Een dergelijke beperking werd bevestigd in het voormelde arrest, waarin het Europees Hof voor de Rechten van de Mens als volgt oordeelde: "*Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. (…) it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context.*"[24]

Hoewel in België een strafrechtelijke aanpak mogelijk is (in tegenstelling tot wat destijds in Finland het geval was), nopen de procedurele impasse omtrent het drukpersmisdrijf en het feit dat de slachtoffers van onwettige anonieme daden op het internet het keuzerecht wordt ontzegd, ertoe de voorgestelde bepaling op te nemen in het Belgisch wetgevingsarsenaal. Het is van wezenlijk belang te beklemtonen dat de voorgestelde regeling zou inhouden dat de identificatie er moet komen na tussenkomst van een onafhankelijke en onpartijdige rechter die zich over het verzoek buigt in het kader van het voormelde streven naar een evenwicht tussen de grondrechten.

Dat verzoek zou door de voorzitter van de rechtbank van eerste aanleg rechtstreeks aan de dienstverleners worden gericht na een eenzijdig verzoekschrift van eender welke belanghebbende partij in de zin van de

[23] Arrest EHRM *K.U. v. Finland*, 2 december 2008, verzoekschrift nr. 2872/02, § 49.

[24] Arrest EHRM *K.U. v. Finland*, 2 december 2008, verzoekschrift nr. 2872/02, § 49.

À cet égard, il y a lieu de constater que la Cour européenne des droits de l'homme, dans son arrêt K.U. c. Finlande, du 2 décembre 2008[23], a estimé qu'une protection pratique et effective d'un mineur, ayant fait l'objet d'une annonce à caractère sexuel sur Internet, impliquait, dans le chef de la Finlande, l'obligation d'adopter des mesures efficaces pour identifier et poursuivre l'auteur.

6.3. ***De l'équilibre à déterminer***

Autoriser la communication d'informations permettant d'agir civilement contre l'auteur d'activités supposées illicites est une limitation nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour assurer le respect des droits et libertés d'autrui.

Une telle limitation a été confirmée par l'arrêt précité dans lequel la Cour européenne des droits de l'homme a précisé: "Même si la liberté d'expression et la confidentialité des communications sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services Internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, cette garantie ne peut être absolue, et elle doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui. (…), le législateur aurait dû en tout cas prévoir un cadre permettant de concilier les différents intérêts à protéger dans ce contexte."[24]

Bien qu'une voie pénale soit prévue en Belgique (contrairement à ce qui était le cas à l'époque en Finlande), l'impasse procédurale rencontrée en matière de délit de presse et la privation du droit optionnel bénéficiant aux victimes d'actes illicites anonymes sur Internet, imposent d'insérer dans l'arsenal législatif belge la disposition proposée. Il est essentiel de souligner que le système proposé prévoit que l'identification résultera nécessairement de l'intervention d'un juge indépendant et impartial qui procédera à l'examen de la demande dans le cadre de la mise en balance des droits fondamentaux précitée.

Cette demande du président, formulée directement auprès des prestataires, interviendrait à l'issue d'une requête unilatérale introduite par toute partie intéressée au sens des articles 17 et 18 du Code judiciaire (Des

[23] Arrêt CEDH, K.U. c. Finlande, 2 décembre 2008, Requête n° 2872/02, § 49.

[24] Arrêt CEDH, K.U. c. Finlande, 2 décembre 2008, Requête n° 2872/02, § 49.

artikelen 17 en 18 van het Gerechtelijk Wetboek (voorwaarden van de rechtsvordering), teneinde die partij de mogelijkheid te bieden, indien het verzoekschrift wordt ingewilligd en indien de dader van de potentieel foute uitlatingen op het internet kon worden geïdentificeerd, een op burgerlijke aansprakelijkheid berustende vordering tegen die dader in te stellen.

Gelet op de inherente dringendheid van dergelijke zaken en op de korte bewaartermijn van persoonsgegevens waaraan de platformverantwoordelijken zich dienen te houden, zal een dergelijke vordering pas effect hebben indien een vermoeden van absolute noodzakelijkheid geldt.

Om de door de CNCDH beschreven risico's uit te weg te gaan en vanuit de logica van een verplichte medewerking van de tussenpersonen, wordt tevens voorgesteld om die tussenpersonen persoonlijk aansprakelijk te stellen voor de betwiste uitingen die op hun platforms worden verspreid, indien zij weigeren over te gaan tot de identificatie die door de voorzitter van de rechtbank van eerste aanleg wordt bevolen. De sancties kunnen in voorkomend geval worden afgestemd op de sancties die in het Belgisch recht moeten worden opgenomen bij de tenuitvoerlegging van de EU-verordeningen 2022/2065 (digitaledienstenverordening) en 2023/1543.

conditions de l'action) afin de permettre à la partie intéressée, s'il est fait droit à l'action et si l'auteur des expressions potentiellement fautives sur Internet a pu être identifié, d'introduire une action en responsabilité civile à son encontre.

Compte tenu de l'urgence inhérente à ce type d'affaires et du court délai de conservation des données personnelles imposé aux responsables des plateformes, une telle action n'aura d'effet que si l'absolue nécessité est présumée.

Afin d'éviter les écueils décrits par la Commission nationale consultative des droits de l'homme en France (CNCDH), et dans la logique de l'obligation de collaboration imposée aux prestataires intermédiaires, il est proposé également de rendre les prestataires intermédiaires personnellement responsables des expressions litigieuses diffusées sur leurs plateformes s'ils refusent l'identification sollicitée par le président du tribunal de première instance. Les sanctions pourront, le cas échéant, être alignées sur celles que le droit belge devra intégrer dans le cadre de l'exécution des Règlements (UE) 2022/2065 (DSA) et (UE) 2023/1543.

Khalil Aouasti (PS)
Hugues Bayet (PS)
Marie Meunier (PS)
Pierre-Yves Dermagne (PS)
Caroline Désir (PS)
Lydia Mutyebele Ngoi (PS)

WETSVOORSTEL

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

Artikel XII.20 van het Wetboek van economisch recht, laatstelijk gewijzigd bij de wet van 21 april 2024, wordt aangevuld met een paragraaf 3, luidende:

"§ 3. Onverminderd eventuele strafrechtelijke en administratieve vervolgingen kan de voorzitter van de rechtbank van eerste aanleg, die optreedt als bevoegde gerechtelijke autoriteit overeenkomstig artikel XII.20, § 2, tweede lid, diezelfde dienstverleners bevelen, na in de mate van het mogelijke een evenwicht te hebben nagestreefd tussen de in het geding zijnde belangen en grondrechten, om alle informatie mee te delen waarover zij beschikken en die nuttig is voor het onderzoek naar en de vaststelling van de fouten die derden via hun diensten hebben begaan, waaronder in het bijzonder de identiteit van die derden. De voorzitter doet een uitspraak met voorrang boven alle andere zaken en op een eenzijdig verzoekschrift van elke belanghebbende partij zoals bedoeld in de artikelen 17 en 18 van het Gerechtelijk Wetboek. Er geldt een vermoeden van absolute noodzakelijkheid. Voor het overige worden de artikelen 1026 tot 1034 van het Gerechtelijk Wetboek toegepast.

Indien de verzochte informatie niet wordt verstrekt binnen de door de voorzitter van de rechtbank van eerste aanleg vastgelegde termijn, zijn de aangezochte dienstverleners persoonlijk aansprakelijk voor de schade die werd geleden als gevolg van de in het eenzijdig verzoekschrift bedoelde betwiste activiteiten."

27 februari 2024

PROPOSITION DE LOI

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2

L'article XII.20. du Code de droit économique, modifié en dernier lieu par la loi du 21 avril 2024, est complété par un paragraphe 3, rédigé comme suit:

"§ 3. Sans préjudice d'éventuelles poursuites pénales ou administratives, le président du tribunal de première instance, agissant en tant qu'autorité judiciaire compétente conformément à l'article XII.20, § 2, alinéa 2, peut ordonner aux mêmes prestataires, après avoir procédé dans la mesure du possible à la mise en balance des intérêts et droits fondamentaux en cause, de communiquer toutes les informations dont ils disposent et qui sont utiles à la recherche et à la constatation des fautes commises par des tiers par leur intermédiaire, dont notamment l'identification de ces tiers. Le président statue toutes affaires cessantes sur requête unilatérale de toute partie intéressée au sens des articles 17 et 18 du Code judiciaire. L'absolue nécessité est présumée. Il est fait, pour le surplus, application des articles 1026 à 1034 du Code judiciaire.

À défaut de fournir les informations sollicitées dans le délai fixé par le président du tribunal de première instance, les prestataires sollicités peuvent être tenus personnellement responsables du préjudice causé par les activités litigieuses visées par la requête unilatérale."

27 février 2024

Khalil Aouasti (PS)
Hugues Bayet (PS)
Marie Meunier (PS)
Pierre-Yves Dermagne (PS)
Caroline Désir (PS)
Lydia Mutyebele Ngoi (PS)

Centrale drukkerij - Imprimerie centrale