

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

6 octobre 2021

PROPOSITION DE LOI

visant à réprimer le “doxing”

(déposée par
Mme Laurence Zanchetta et consorts)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

6 oktober 2021

WETSVOORSTEL

tot beteugeling van “doxing”

(ingediend door
mevrouw Laurence Zanchetta c.s.)

RÉSUMÉ

La présente proposition de loi vise à incriminer le “doxing”, qui peut être défini comme le fait de révéler des informations personnelles sur un tiers avec une intention malveillante.

SAMENVATTING

Dit wetsvoorstel strekt ertoe doxing strafbaar te stellen. Doxing kan worden omschreven als het met kwade bedoelingen onthullen van persoonlijke informatie over een derde.

N-VA	: Nieuw-Vlaamse Alliantie
Ecolo-Groen	: Ecologistes Confédérés pour l'organisation de luttes originales – Groen
PS	: Parti Socialiste
VB	: Vlaams Belang
MR	: Mouvement Réformateur
CD&V	: Christen-Democratisch en Vlaams
PVDA-PTB	: Partij van de Arbeid van België – Parti du Travail de Belgique
Open Vld	: Open Vlaamse liberalen en democraten
Vooruit	: Vooruit
cdH	: centre démocrate Humaniste
DéFI	: Démocrate Fédéraliste Indépendant
INDEP-ONAFH	: Indépendant - Onafhankelijk

<i>Abréviations dans la numérotation des publications:</i>		<i>Afkorting bij de numerering van de publicaties:</i>	
DOC 55 0000/000	Document de la 55 ^e législature, suivi du numéro de base et numéro de suivi	DOC 55 0000/000	Parlementair document van de 55 ^e zittingsperiode + basisnummer en volgnummer
QRVA	Questions et Réponses écrites	QRVA	Schriftelijke Vragen en Antwoorden
CRIV	Version provisoire du Compte Rendu Intégral	CRIV	Voorlopige versie van het Integraal Verslag
CRABV	Compte Rendu Analytique	CRABV	Beknopt Verslag
CRIV	Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)	CRIV	Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)
PLEN	Séance plénière	PLEN	Plenum
COM	Réunion de commission	COM	Commissievergadering
MOT	Motions déposées en conclusion d'interpellations (papier beige)	MOT	Moties tot besluit van interpellaties (beigegekleurig papier)

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

Le “doxing” peut se définir, de manière générale, comme un usage malveillant des données à caractère personnel. Issu de l’anglais “document tracing” (en français: traçage de document), le *doxing* désigne le fait de révéler des informations personnelles sur un tiers avec une intention malveillante. Le moment venu, les informations personnelles sont dévoilées publiquement, notamment sur les réseaux sociaux, dans le but de nuire.

Souvent, le fait d’exposer publiquement les données personnelles d’une victime (son nom, son adresse, son numéro de téléphone, mais aussi dans certains cas des informations sur sa famille, des mots de passe, son numéro de carte bancaire), poursuit l’objectif d’humilier la personne et/ou de la rendre vulnérable aux attaques de tiers – que ces attaques prennent ensuite la forme d’injures, de harcèlement, voire de violence physique.

Le *doxing* peut, dès lors, causer un préjudice sérieux et persistant à la victime, notamment dans certains cas extrêmes où l’irruption des informations personnelles dans la sphère publique génère une attaque groupée, une attaque en meute contre la personne prise pour cible.

Ainsi, en juin 2019, l’identité d’un assistant et docteur de l’Université de Gand qui tenait un compte Twitter critique sur le groupe d’extrême droite “Schild & Vrienden”, a été tracée et dévoilée par des utilisateurs sur le forum Internet 4chan. À la suite de la publication d’informations personnelles (identité, adresse IP, numéro de téléphone...), l’homme s’est retrouvé la cible d’une véritable campagne de haine ainsi que de menaces de mort proférées à son égard¹.

De même, en 2017, la journaliste Nadia Daam a été “doxée” à la suite d’une chronique sur Europe 1 où elle affirmait son soutien à deux victimes de cyberharcèlement. L’adresse de son domicile et du collègue de sa fille ont été divulguées; la journaliste a dû quitter son appartement pendant plusieurs jours sur les conseils de la police, étant donné le déferlement d’insultes, de menaces, voire d’appels au viol et au meurtre qu’elle subissait².

¹ “Commotie over haatcampagne tegen Schild & Vrienden-criticus” in *De Tijd*, 5 juin 2019.

² “Je vais t’égorger et violer ton cadavre”, in *Le Monde*, 6 mai 2018.

TOELICHTING

DAMES EN HEREN,

Doxing kan algemeen worden omschreven als de kwaadwillige aanwending van persoonsgegevens. De term is afkomstig van het Engelse “document tracing” (dus de opsporing van documenten) en verwijst naar het met kwade bedoelingen onthullen van persoonlijke informatie over een derde. Op een gegeven ogenblik wordt die persoonlijke informatie openbaar gemaakt, in het bijzonder via de sociale media, met de bedoeling schade te berokkenen.

Vaak worden de persoonsgegevens van een slachtoffer (naam, adres, telefoonnummer, maar soms ook gegevens over gezinsleden, wachtwoorden, bankkaartnummers enzovoort) openbaar gemaakt om het slachtoffer te vernederen en/of om het kwetsbaar te maken voor aanvallen door derden (in de vorm van beledigingen, stalking en zelfs fysiek geweld).

Doxing kan het slachtoffer derhalve ernstige en blijvende schade toebrengen. Dat geldt in het bijzonder in bepaalde extreme gevallen waarin het openbaar worden van persoonlijke informatie leidt tot een aanval door een groep en waarbij een doelwit wordt opgejaagd door een meute.

Zo werd in juni 2019 de identiteit van een assistent en doctoraalstudent van de Universiteit Gent, die zich op zijn Twitteraccount kritisch uitliet over de extreemrechtse groepering Schild & Vrienden, opgespoord en openbaar gemaakt door gebruikers van het internetforum 4chan. Na de openbaarmaking van zijn persoonsgegevens (naam, IP-adres, telefoonnummer enzovoort) is de man het doelwit geworden van een regelrechte haatcampagne en zijn bovendien zelfs doodsbedreigingen tegen hem geuit¹.

In 2017 kreeg ook journaliste Nadia Daam te maken met doxing, na een opiniebijdrage op de Franse radiozender *Europe 1*, waarin ze haar steun betuigde aan twee slachtoffers van cyberpesten. Haar thuisadres en dat van de school van haar dochter werden bekendgemaakt, en wegens de stortvloed aan beledigingen, bedreigingen en zelfs oproepen tot verkrachting en moord die ze over zich heen kreeg, moest zij op advies van de politie enkele dagen haar appartement verlaten².

¹ “Commotie over haatcampagne tegen Schild & Vrienden-criticus”, *De Tijd*, 5 juni 2019.

² “Je vais t’égorger et violer ton cadavre”, *Le Monde*, 6 mei 2018.

Fréquente dans le champ des violences sexuelles et sexistes, caractéristique d'une "nouvelle génération de militance d'extrême droite en ligne"³, cette pratique de mise au pilori numérique a cependant un champ de développement plus large encore. Selon l'association e-enfance, le *doxing* est un fait de cyberharcèlement qui se produit fréquemment en milieu scolaire⁴.

Selon une étude quantitative menée par quatre chercheurs américains⁵, trois types de personnes sont régulièrement visés: les hackers, les passionnés de jeux vidéo et les célébrités. L'âge des victimes est très variable, de 10 à 74 ans, avec une moyenne située autour de 21 ans⁶.

Dans le monde contemporain, les technologies de l'information sont omniprésentes. Elles offrent une merveilleuse opportunité d'expression, pour analyser le monde dans lequel on vit, défendre ses opinions, s'indigner de ce qui mérite de l'être, etc. Malheureusement, ces technologies peuvent également être l'occasion d'abus, notamment lorsqu'elles sont utilisées dans l'objectif de nuire à l'intégrité morale ou physique d'un individu.

Dès lors, il est important qu'un juste équilibre soit établi, pour protéger tant la liberté d'expression et l'accès à l'information que l'intégrité morale et physique des personnes.

Règlement général de protection des données (RGPD) et *doxing*

Le champ d'application du RGPD, s'il est très large, ne concerne pas tout usage de données à caractère personnel. Son article 2.1 en détermine le champ d'application matériel ainsi: "les traitements de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer

³ Assemblée nationale, Commission d'enquête sur la lutte contre les groupuscules d'extrême-droite en France, audition de M. Tristan Mendès France, enseignant au Celsa, maître de conférences associé à Paris Diderot, jeudi 7 mars 2019. Document disponible en ligne: <http://www.assemblee-nationale.fr/15/cr-celgroued/18-19/c1819012.asp>.

⁴ Emmanuelle Piquet, *Le harcèlement scolaire en 100 questions*, Tallandier, Paris, 2017.

⁵ P. Snyder, Ch. Kanich, P. Doerfler, D. McCoy, *Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing*, in IMC, London, November 2017. Document disponible en ligne à l'adresse: <https://www.cs.uic.edu/~psnyder/static/papers/fifteen-minutes.pdf>.

⁶ "Doxing: pourquoi certains internautes divulguent les données privées de leur cible", in *Le Monde*, 21 novembre 2017. Document disponible en ligne: https://www.lemonde.fr/pixels/article/2017/11/21/doxing-pourquoi-certains-internautes-divulguent-les-donnees-privees-de-leurs-cibles_5218143_4408996.html.

Die praktijk waarbij iemand digitaal aan de schandpaal wordt genageld, houdt vaak verband met seksueel en seksistisch geweld dat kenmerkend zou zijn voor een nieuwe generatie van online opererende extreemrechtse militanten³, maar ontwikkelt zich ook buiten die sfeer. Volgens de vereniging e-enfance is doxing een vorm van cyberstalken die vaak voorkomt op school⁴.

Volgens een kwantitatieve studie van vier Amerikaanse onderzoekers zijn mensen uit drie categorieën regelmatig het slachtoffer van doxing: hackers, liefhebbers van videospellen en beroemdheden⁵. De leeftijd van de slachtoffers is heel divers, namelijk van 10 tot 74 jaar, met een gemiddelde van om en bij de 21 jaar⁶.

De informatietechnologie is in de hedendaagse samenleving alomtegenwoordig. Ze biedt fantastische mogelijkheden om zich uit te drukken, om onze leefwereld te ontleden, om meningen te verdedigen, om verontwaardiging te uiten wanneer dat gerechtvaardigd is enzovoort. Helaas kunnen die technologieën ook aanleiding geven tot misbruik, meer bepaald wanneer ze louter en alleen worden gebruikt met de bedoeling schade te berokkenen aan de geestelijke of fysieke integriteit van mensen.

Derhalve moet een goede balans tot stand worden gebracht, teneinde zowel de vrijheid van meningsuiting en de toegang tot informatie, als de geestelijke en lichamelijke integriteit van de burgers te beschermen.

De algemene verordening gegevensbescherming (AVG) en doxing

De toepassingsfeer van de AVG is weliswaar heel breed, maar bestrijkt niet elk gebruik van persoonsgegevens. In artikel 2.1 ervan wordt de materiële toepassingsfeer ervan bepaald als volgt: "Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen

³ *Assemblée nationale, Commission d'enquête sur la lutte contre les groupuscules d'extrême droite en France*, hoorzitting met de heer Tristan Mendès France, docent bij Celsa (*Centre d'Etudes Littéraires et Scientifiques Appliquées*), lector bij Paris Diderot, donderdag 7 maart 2019. Zie: <http://www.assemblee-nationale.fr/15/lcr-celgroued/18-19/lc1819012.asp>.

⁴ Emmanuelle Piquet, *Le harcèlement scolaire en 100 questions*, Tallandier, Parijs, 2017.

⁵ P. Snyder, Ch. Kanich, P. Doerfler, D. McCoy, *Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing*, IMC, Londen, november 2017. Zie: <https://www.cs.uic.edu/~psnyder/static/papers/fifteen-minutes.pdf>.

⁶ "Doxing: pourquoi certains internautes divulguent les données privées de leur cible", *Le Monde*, 21 novembre 2017. Zie: https://www.lemonde.fr/pixels/article/2017/11/21/doxing-pourquoi-certains-internautes-divulguent-les-donnees-privees-de-leurs-cibles_5218143_4408996.html.

dans un fichier”. Autrement dit, le RGPD s’applique à la gestion regroupée de données à caractère personnel.

Or le *doxing* peut très bien concerner une information privée qui n’a pas vocation à se retrouver dans un fichier. Par exemple, une personne malveillante peut suivre sa victime jusqu’à son domicile afin d’en divulguer l’adresse sur internet. Cette personne malveillante n’a pas fait usage d’un fichier ou d’une donnée appelée à être inscrite dans un fichier pour atteindre son objectif.

Une proposition inspirée de la loi française

En France, l’assassinat de l’enseignant Samuel Paty en octobre 2020 fut l’une des raisons de l’adoption d’une disposition spécifique dans le Code pénal français. Pour rappel, cet enseignant fut assassiné à la suite de la révélation de son identité sur les réseaux sociaux dans un contexte d’incitation à la violence à son endroit.

Les auteurs de la présente proposition de loi reprennent la nouvelle incrimination française en y apportant certaines adaptations. L’incrimination proposée ne vise que les risques à la personne et non pas aux biens. D’autre part, il est également précisé, dans l’article même, que cette incrimination ne peut pas avoir pour effet de porter atteinte à la liberté d’information.

Il est dès lors prévu de punir toute personne qui diffuse ou transmet des informations concernant une personne aux fins de l’exposer, elle ou sa famille, à un risque direct contre sa personne.

L’infraction vise la divulgation d’informations dans le but d’exposer une personne à un risque direct et ne concerne ainsi pas la révélation d’éléments dans le but d’informer le public – même si ces éléments peuvent ensuite être repris par des tiers dans le but d’exposer des personnes à un risque.

Si le phénomène du “*doxing*” a pris une ampleur sans précédent avec l’essor des réseaux sociaux, les auteurs de la présente proposition de loi ne souhaitent pas limiter la portée de cette nouvelle incrimination au seul espace dématérialisé qu’est internet. La communication d’information de nature privée dans un but malveillant

of die bestemd zijn om daarin te worden opgenomen.”. De AVG is dus van toepassing op het gegroepeerde beheer van persoonsgegevens.

Doxing kan echter ook betrekking hebben op privéinformatie die niet bestemd is om in een bestand te worden opgenomen. Iemand met kwade bedoelingen kan bijvoorbeeld zijn slachtoffer volgen tot diens woonst, teneinde het adres ervan te verspreiden op het internet. Om zijn doel te bereiken, maakt die kwaadwillige geen gebruik van een bestand of van vooropname in een bestand bestemde informatie.

Een voorstel geïnspireerd door de Franse wetgeving

In Frankrijk vormde de moord op leerkracht Samuel Paty in oktober 2020 een van de redenen om een specifieke bepaling op te nemen in het Franse strafwetboek. Ter herinnering: die leerkracht werd vermoord ten gevolge van de onthulling van zijn identiteit op de sociale media, in een sfeer die aanzette tot geweld jegens hem.

In dit wetsvoorstel wordt de nieuwe Franse strafbaarstelling overgenomen, zij het met een aantal aanpassingen. De voorgestelde strafbaarstelling behelst alleen de risico’s voor personen en niet die voor goederen. Voorts wordt beoogd in het artikel zelf eveneens aan te geven dat deze strafbaarstelling niet mag leiden tot een schending van de vrijheid van informatie.

Derhalve is het de bedoeling dat een straf wordt ingevoerd voor eenieder die informatie over een persoon verspreidt of doorgeeft, met als doel de betrokkene of diens gezinsleden bloot te stellen aan een direct risico jegens hun persoon.

Het misdrijf betreft de verspreiding van informatie teneinde iemand aan een direct risico bloot te stellen en dus niet de onthulling van elementen met als doel het publiek te informeren, zelfs indien die aspecten vervolgens door derden kunnen worden misbruikt om de betrokkenen aan een risico bloot te stellen.

Doxing heeft weliswaar ongeziene proporties aangenomen door het succes van de sociale media, maar de indieners van dit wetsvoorstel willen de toepassings sfeer van deze nieuwe strafbaarstelling niet beperken tot louter het immateriële internet. Het wetsvoorstel strekt ertoe dat een en ander van toepassing zou zijn op het met

par tout moyen entre ainsi dans le champ d'application de la présente proposition de loi.

Laurence ZANCHETTA (PS)
Khalil AOUASTI (PS)
Patrick PRÉVOT (PS)
Chanelle BONAVENTURE (PS)
Leslie LEONI (PS)
Christophe LACROIX (PS)

kwade bedoelingen meedelen van privéinformatie via om het even welk kanaal.

PROPOSITION DE LOI

Article 1^{er}

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

Art. 2

Dans le code pénal, il est inséré un article 327*bis* rédigé comme suit:

“Art. 327*bis*. Quiconque aura révélé, diffusé ou transmis, par quelque moyen que ce soit, des informations relatives à la vie privée, familiale ou professionnelle d'une personne permettant de l'identifier ou de la localiser aux fins de l'exposer ou d'exposer les membres de sa famille à un risque direct d'atteinte à leur intégrité que l'auteur ne pouvait ignorer, sera puni d'un emprisonnement d'un mois à trois ans et d'une amende de 100 à 5 000 euros.

Les dispositions de l'alinéa 1^{er} n'ont pas pour objet et ne peuvent avoir pour effet de réprimer la révélation ou la diffusion de faits, de messages, de données, de sons ou d'images qui ont pour but d'informer le public alors même que ces informations pourraient ensuite être reprises et retransmises par des tiers dans le but de nuire à la personne qu'elles permettent d'identifier ou de localiser.”

20 septembre 2021

Laurence ZANCHETTA (PS)
Khalil AOUASTI (PS)
Patrick PRÉVOT (PS)
Chanelle BONAVENTURE (PS)
Leslie LEONI (PS)
Christophe LACROIX (PS)

WETSVOORSTEL

Artikel 1

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

Art. 2

In het Strafwetboek wordt een artikel 327*bis* ingevoegd, luidende:

“Art. 327*bis*. Hij die door om het even welk middel informatie heeft verspreid of doorgegeven over de persoonlijke levenssfeer, het gezinsleven of het beroepsleven van iemand en het aldus mogelijk heeft gemaakt hem te herkennen of te lokaliseren, met als doel hem of zijn gezinsleden rechtstreeks bloot te stellen aan een schending van hun integriteit, waarbij dat risico door de dader gekend had moeten zijn, wordt gestraft met gevangenisstraf van één maand tot drie jaar en met geldboete van honderd euro tot vijfduizend euro.

De bepalingen in het eerste lid strekken er niet toe en mogen niet tot gevolg hebben dat de onthulling of verspreiding wordt beteugeld van feiten, boodschappen, gegevens, geluidsopnamen of beelden die bestemd zijn om het publiek te informeren, zelfs wanneer die informatie nadien kan worden hergebruikt en doorgegeven door derden, met als doel schade toe te brengen aan diegene die via die informatie kan worden herkend of gelokaliseerd.”

20 september 2021