

Geachte minister Grapperhaus,

1. Bits of Freedom maakt graag van de gelegenheid gebruik om te reageren op het conceptwetsvoorstel Strafbbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden.¹ In onze reactie zullen we eerst kort ingaan op het beoogde doel van het voorstel, dan benoemen we enkele onderliggende problemen die aandacht behoeven en tenslotte bespreken we nog een aantal specifieke details van het voorstel.

Doel van het voorstel

2. Om te beginnen willen we u graag complimenteren met het voorstel. Het tegengaan van de verspreiding van persoonsgegevens voor intimiderende doeleinden, is belangrijk. We leven in een maatschappij waarin het helaas vaak heel makkelijk is om aan persoonsgegevens van derden te komen. Dat geldt ook voor de verspreiding van deze gegevens in opruiende berichten. Ook wij zien dat dit vaak gebeurt met intimidatie als oogmerk. Voor slachtoffers kan deze intimidatie zeer grote consequenties hebben, waarbij het slachtoffer zich niet meer veilig voelt. We delen ook het standpunt dat de huidige strafbaarstellingen niet afdoende zijn. Het is daarom goed dat het kabinet een nieuwe strafbaarstelling wil introduceren. In onze ogen is daarbij ook een redelijke balans gevonden tussen de bescherming van de persoonlijke levenssfeer aan de ene kant en de bescherming de vrijheid van meningsuiting aan de andere kant.

Meer structurele problemen

3. Het is van belang naast de introductie van deze strafbaarstelling niet alle onderliggende problemen adresseert. Deze strafbaarstelling probeert dat ook niet. Maar dat neemt niet weg dat het belangrijk is om naast de introductie van deze strafbaarstelling ook oog te hebben voor die meer structurele problemen. Het verkleinen van deze meer structurele problemen, beperkt ook de mogelijkheden tot en de impact van misbruik van gegevens. We lichten hier graag twee van deze problemen uit.
 - a. Veel te vaak zijn persoonsgegevens beschikbaar in publiek toegankelijke bronnen. Het register van de Kamer van Koophandel is daar een goed voorbeeld van. Als zelfstandig ondernemer zal het vestigingsadres vaak overeenkomen met het woonadres van de ondernemer. Met de publiek toegankelijke registratie hiervan, is het privéadres eenvoudig opvraagbaar. Een ander voorbeeld is het Kadaster, waarin gegevens zoals iemands adres, burgerlijke staat en financiële gegevens openbaar toegankelijk zijn. In beide gevallen kunnen zulke gegevens, al dan niet in combinatie met andere gegevens uit andere bronnen, gebruikt worden voor intimiderende doeleinden. Het beperken van de beschikbaarheid van dit soort gegevens draagt bij aan de beperking van het mogelijke misbruik ervan.

¹ <https://internetconsultatie.nl/strafbaarstellinggebruikpersoonsgegevensvoorintimiderendedoeleinden/>

- b. U merkt terecht op dat er in het huidige maatschappelijke klimaat sprake is van een verharding van uitingen op het internet. Onze publieke debat online is sterk afhankelijk van de technologie die we daarvoor gebruiken. Op het moment wordt het publieke debat online hoofdzakelijk gevoerd via een beperkt aantal platforms van een nog beperkter aantal Amerikaanse technologiebedrijven. De dominantie van Facebook, en enkele andere partijen in het online publieke debat, maakt dat zij grote invloed hebben op de inhoud van ons publieke debat. Maar wellicht nog relevanter is dat deze platforms ook nog eens de vorm van het gesprek bepalen, door allerlei keuzes in het ontwerp van het platform. De berichtjes op Twitter zijn door hun beperkte lengte en de retweet-counter eronder, weinig uitnodigend om een genuanceerd verhaal te vertellen. En het belang om van platformen om de aandacht van gebruikers zo lang mogelijk vast te houden, maakt dat deze platforms bepaald gedrag bevorderen en ander gedrag juist ontmoedigen. Het gevolg is dat radicaler berichtjes makkelijk *viral* kunnen gaan, terwijl voor een genuanceerder verhaal geen plaats is. Daar is in 2021 in opdracht van Bits of Freedom uitgebreid onderzoek naar gedaan door Holly Robins.²

Strafbaarstelling

4. Meer inhoudelijk hebben we enkele vragen en opmerkingen. In de eerste plaats behoeven enkele begrippen een nadere toelichting.
- a. Het begrip “identificerend persoonsgegevens” wijkt af van de definitie in de Algemene Verordening Gegevensbescherming. Volgens de definitie in deze verordening zijn persoonsgegevens “alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon”. Er bestaan in dat licht dan ook geen persoonsgegevens die niet ook identificerend zijn. Mogelijk bedoelde u met het begrip “identificerend persoonsgegevens” iets anders, maar dan wordt uit de voorgestelde wetstekst of toelichting niet duidelijk wat u dan precies bedoeld. Het kan ook betekenen dat u wél dezelfde soort gegevens bedoeld. Als dat het geval is, raden wij u aan om de term “persoonsgegeven” te gebruiken, al dan niet met een verwijzing naar de Algemene Verordening Gegevensbescherming.
- b. Het begrip “vrees aanjagen” is onvoldoende helder gedefinieerd. Wanneer is er precies sprake van vrees aanjagen? Het gaat daarbij, volgens de toelichting, om “een emotie, die ieder normaal mens onder vergelijkbare omstandigheden ook zou hebben.” Valt, bijvoorbeeld, het aankaarten van het feit dat de directeur van Shell privé een groot stuk grond heeft gekocht in een land waar het bedrijf is veroordeeld voor grootschalige vervuiling ook onder “vrees aanjagen”? Is het hebben van angst dat er activisten met bootjes rondom het eiland varen zo’n emotie? Is het hebben van een angst op publicitaire schade een reden voor strafbaarheid van de uiting? We adviseren u dit beter uit te leggen.
- c. In het verlengde daarvan is “ernstige hinder van de uitoefening van ambt of beroep” onvoldoende genuanceerd. In de toelichting beschrijf u het voorbeeld van

² “Performing the Platform: A Taxonomy of Content Manipulation”, Dr. Holly Robbins, februari 2021

het verspreiden van persoonsgegevens van undercoveragenten. Deze agenten zouden dan hun werk niet meer goed kunnen doen. Het zou daarom noodzakelijk zijn om deze handeling strafbaar te stellen. Daar is misschien iets voor te zeggen in de context van een groot opsporingsonderzoek naar criminele activiteiten. Maar in een context waarin undercoveragenten deelnemen aan een demonstratie voor, bijvoorbeeld, een beter milieu of gelijke rechten voor mensen met kleur, is zo'n strafbaarstelling problematisch. We adviseren u dit nader uit te werken.

- d. Het voorbeeld van undercoveragenten is voor het overige ook onhandig. Leidt de verspreiding van identificerende gegevens van undercoveragenten niet altijd tot een aanmerkelijke kans dat de identiteit van de agenten kan worden achterhaald dan wel onthuld en dat deze agenten daardoor gedwongen zouden kunnen worden hun (undercover)werkzaamheden na te laten? Als dat zo is, dan is er toch altijd al sprake van ambtswang en is dat reeds strafbaar? En is er dan wel sprake van intimidatie? Of is er dan niet gewoon sprake van “uit de anonimiteit halen” en daarmee het teniet doen van de effectiviteit van een opsporingsmiddel? Het lijkt ons niet wenselijk om het ondermijnen van de effectiviteit van opsporingsmiddelen door de verspreiding van gegevens als zodanig strafbaar te laten zijn.
- e. Bits of Freedom gaat er vanuit dat een platform, via welke een gebruiker van het platform persoonsgegevens van een derde verspreid, met het oogmerk om deze derde vrees aan te jagen, niet strafbaar gehouden kan worden op grond van dit artikel. Is dat juist?
- f. Het is ons niet duidelijk waarom er een expliciet onderscheid is gemaakt tussen “het een ander vrees aanjagen” en het “hem in de uitoefening van zijn ambt of beroep ernstig te hinderen”. We nemen aan dat bedoeld wordt dat iemand ernstig gehinderd wordt in de uitoefening van zijn ambt of beroep doordat de verspreiding van persoonsgegevens als intimiderend ervaren wordt. Als dat zo is, is er dan niet ook al sprake van “het aanjagen van vrees”? De scheiding van deze contexten is kunstmatig, ook omdat intimidatie in privésfeer zonder twijfel ook impact heeft op de uitoefening van iemands ambt of beroep en omgedraaid. Zonder een nadere uitleg van noodzakelijkheid raden wij u aan dit te vereenvoudigen.

Uitzonderingsgronden

- 6. Er zijn twee, cumulatieve, voorwaarden om aan de uitzonderingsgrond van het tweede lid te voldoen: “te goeder trouw handelen” en “in het algemeen belang”. Is het niet ook mogelijk om wél “te goeder trouw te handelen”, maar niet “in het algemeen belang”? Is dat niet een situatie die ook bescherming behoeft? Het zou ook kunnen betekenen dat “van iemand die een ander onbewust of onopzettelijk doet schrikken of hindert in diens privacy-genot [gezegd zou kunnen worden] dat hij vrees aanjaagt.” Iets dat u eerder expliciet wilde voorkomen.³ Wij raden u aan om in het voorstel de frase “in het algemeen belang” te schrappen.

³ Tweede Kamer, vergaderjaar 1998–1999, 25 768, nummer 7, pagina 15

7. In de toelichting op het tweede lid wordt hoofdzakelijk of alleen gesproken over de bescherming die journalisten of klokkenluiders zouden moeten kunnen genieten. Dat deze groepen beschermd moeten worden is evident. Het moet echter duidelijk zijn dat ook andere groepen aanspraak moeten kunnen maken op deze bescherming, we denken daarbij bijvoorbeeld aan burgerjournalisten of activisten die onderzoek doen naar misstanden. Wij raden u aan dit duidelijker te verwoorden in het voorstel.

Wij hopen u hiermee voldoende te hebben geïnformeerd. Vanzelfsprekend zijn wij graag bereid tot een nadere toelichting, mocht daaraan behoefte bestaan.

Met vriendelijke groet,