Samenvatting

Grondrechten, zoals het recht op privacy, zijn primair gericht op het beschermen van de burger tegen de staat. Maar ook tussen burgers onderling kunnen (ernstige) aantastingen van grondrechten plaatsvinden. Om die reden is het van belang om te onderzoeken in hoeverre grondrechten, meer in het bijzonder het recht op privacy, ook bescherming bieden in 'horizontale verhoudingen'. In de initiatiefnota onderlinge privacy van het Tweede Kamerlid Koopmans (wordt het probleem van privacyschendingen in horizontale verhoudingen gesignaleerd. Met privacyschendingen in horizontale verhoudingen wordt gedoeld op privacyschendingen tussen burgers onderling en tussen burgers en rechtspersonen (bedrijven, verenigingen et cetera). Horizontale privacybescherming onderscheidt zich daarmee van de verticale privacybescherming, die betrekking heeft op de relatie burger-overheid.

In dit onderzoek staat een drieledige probleemstelling centraal:

- Wat kan Nederland leren van de wijze waarop de horizontale privacy in andere Europese landen is beschermd?
- In hoeverre zijn deze oplossingen inpasbaar in de Nederlandse context?
- Zijn er onwenselijk geachte effecten of neveneffecten te verbinden aan deze mogelijkheden voor een betere horizontale privacybescherming in Nederland?

De landen die zijn betrokken in de rechtsvergelijking zijn: Duitsland, Polen, Zweden en het Verenigd Koninkrijk.

Om de probleemstelling te beantwoorden is een antwoord gezocht op de volgende vragen:

- Wat is 'horizontale privacy' en hoe wordt deze in Nederland en de onderzochte landen genormeerd?
- Wat zijn de te beschermen belangen die in het geding kunnen zijn bij aantasting van de horizontale privacy?
- Welke aantastingen van deze belangen zijn er momenteel?
- Hoe is de bescherming van de horizontale privacy vormgegeven?
- Welke vormen van preventie, handhaving en vervolging van schendingen worden gehanteerd?
- Welke samenwerkingsvormen tussen burgers, bedrijven en overheid bestaan er om horizontale privacyschendingen tegen te gaan?
- Hoe is de horizontale privacybescherming vormgegeven in Duitsland, Polen, Zweden en het Verenigd Koninkrijk?
- In hoeverre zijn nuttige beschermingsmaatregelen uit deze landen in te passen in de Nederlandse context?
- Wat zijn eventuele negatieve effecten van de invoering van maatregelen om de horizontale privacy beter te beschermen?

De scope van dit onderzoek is beperkt tot 'digitale' schendingen van de privacy. In het onderzoek richten wij ons op de relatie burger-burger en de relatie burger-private rechtspersoon (meer specifiek burger-bedrijfsleven). Wel ligt de nadruk op het bespreken en analyseren van privacyschendingen tussen burgers onderling.

Horizontale privacyschendingen

De privacy van burgers kan in horizontale verhoudingen op allerlei manieren worden geschonden. In ons onderzoek hebben wij een onderscheid gemaakt tussen de handelingen waardoor privacy kan worden geschaad en de gevolgen die dit kan hebben voor het individu en de samenleving als geheel (de waarden en belangen die daardoor worden aangetast).

Handelingen die de privacy kunnen aantasten zijn: observeren, het verzamelen en vastleggen van gegevens, analyse en besluitvorming, creëren, delen en openbaarmaken van gegevens en het interacteren en communiceren met personen.

Observeren
Schendingen van de privacy beginnen meestal met het observeren van personen en hun gedrag. In het digitale tijdperk gaat het dan niet alleen om het bekijken van een persoon (al dan niet met technische hulpmiddelen), maar ook om het volgen van een persoon op sociale media en het bekijken van iemands gedragingen op het internet.

Verzamelen en vastleggen
Observeren gaat vaak hand in hand met het daadwerkelijk verzamelen en vastleggen van (persoons)gegevens. Denk aan het opnemen van beelden of gesprekken met een mobiele telefoon, maar ook aan het vastleggen van verkeersgegevens of de locatie van een persoon.

Analyseren en beslissen
Afhankelijk van het doel kunnen vastgelegde gegevens worden geanalyseerd. Deze stap is met name relevant in de verhouding tussen burgers en bedrijven, omdat het bovenal bedrijven zijn die persoonsgegevens analyseren en op basis daarvan (geautomatiseerd) beslissen. Het doel daarvan is doorgaans het inzicht krijgen in het gedrag en de wensen van consumenten.

Creëren
Naast het observeren en vastleggen van gegevens, kunnen gegevens over personen ook worden gecreëerd. Het gaat dan bijvoorbeeld om het maken van foto-montages, *cartoons* en *memes*. Een ander voorbeeld is het doen van uitingen en deze toeschrijven aan een persoon die deze niet heeft gedaan.

Delen en openbaarmaken
Bij veel horizontale privacyschendingen is er sprake van het delen van gegevens (foto's, tekst, video's, geluid). Gegevens kunnen worden gedeeld met één persoon, een (relatief) beperkte groep (een afgesloten WhatsApp groep), of met een grote en in beginsel ongedefinieerde groep (Facebook, Instagram, Twitter). Door het delen van gegevens wordt informatie over een persoon, of de identiteit van een persoon, (ongewenst) openbaar.

Interactie en communicatie
Directe interactie en communicatie kan ook de privacy van personen aantasten. Via digitale communicatiemiddelen is het mogelijk om personen op elk moment te bereiken en met hen, of over hen te communiceren. Afhankelijk van de aard en de frequentie van de communicatie kan deze interactie leiden tot een schending van de privacy. Denk bijvoorbeeld aan *stalking*, cyberpesten, belediging en bedreiging.

Waarden en belangen

Het recht op privacy is een veelomvattend recht. Niet alleen is de reikwijdte van het recht op privacy groot, ook staat het als 'koepelrecht' ten dienste van uiteenlopende waarden en belangen. In ons onderzoek hebben wij de volgende waarden en belangen onderscheiden: de eer en goede naam, vertrouwelijkheid en controle, persoonlijke autonomie, ontwikkeling van de eigen identiteit en emotionele ontlading, het onderhouden van (intieme) relaties, veiligheid, economische gelijkwaardigheid en het voorkomen van hinder.

Eer en goede naam
De eer en goede naam (de reputatie) vormen een onderdeel van het recht op privacy zoals dat is vastgelegd in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM). Onder 'eer' wordt verstaan de waarde die men in zijn of haar eigen ogen heeft. 'Goede naam' doelt op de waarde die men in de ogen van anderen heeft en ziet dus op de reputatie.

Vertrouwelijkheid en controle
Een kernelement van het recht op privacy is de mogelijkheid om de toegang tot de persoonlijke levenssfeer (waaronder begrepen gegevens en communicatie) af te sluiten voor anderen. Deze controle over de persoonlijke levenssfeer stelt ons niet alleen in staat om ons tijdelijk te onttrekken aan sociale interactie, het stelt ons ook in staat om selectief te kunnen zijn in het delen van informatie en aspecten van onze persoonlijkheid. Vertrouwelijkheid en controle spelen ook een rol in de relatie tussen personen en rechtspersonen. Wanneer bedrijven bijvoorbeeld persoonsgegevens verzamelen over personen dan verliezen deze personen daar (grotendeels) de controle over.

Persoonlijke autonomie
Privacy is een belangrijk vereiste voor het behoud van de persoonlijke autonomie. Naarmate derden meer weten over een persoon (diens interesses, zwaktes, voorkeuren, gewoontes, contacten *et cetera*) wordt het makkelijker om macht uit te oefenen over deze persoon, of deze te manipuleren. De persoonlijke autonomie kan in de relatie tussen burger en bedrijf met name in het geding zijn daar waar het gaat om personeel.

Ontwikkeling van de eigen identiteit en emotionele ontlading
Een meer specifiek element van de persoonlijke autonomie is de mogelijkheid om zonder de dwingende ogen van derden de eigen identiteit vorm te geven. Het recht op privacy creëert ruimte om te experimenteren met onze eigen identiteit en (tijdelijk) te ontkomen aan de druk van sociaal wenselijk of verwacht gedrag.

Onderhouden van (intieme) relaties
Vertrouwelijkheid is een voorwaarde voor sociale en maatschappelijke relaties en instituten. Vriendschapsbanden worden bijvoorbeeld voor een groot deel gevormd door exclusieve informatieoverdracht.

Een ander aspect van het recht op privacy dat bij relaties een rol speelt is de zogenaamde *associatieve privacy*. Associatieve privacy heeft betrekking op de relaties en contacten die we onderhouden. Wanneer onze contacten openbaar worden gemaakt, zeker wanneer dit zonder context plaatsvindt, bemoeilijkt het onderhouden van contacten in de toekomst.

Veiligheid
In de meest extreme vormen kunnen horizontale privacyschendingen ook een bedreiging vormen voor de veiligheid van het slachtoffer of diens gevoel van veiligheid. Hierbij kan gedacht worden aan onder andere belediging, bedreiging, belaging (*stalking*) en cyberpesten.

Economische gelijkwaardigheid
Daar waar het gaat over de relatie tussen (potentiële) klant en bedrijf is met name de economische positie van de klant in het geding bij privacyschendingen. Informatie asymmetrie geeft bedrijven een dominante positie ten opzichte van de consument. Deze positie kan onder andere misbruikt worden voor prijsdiscriminatie of het *nudgen* van klanten richting bepaalde productgroepen.

Het voorkomen van hinder
Het voorkomen van hinder is ook een belang dat door het recht op privacy en gegevensbescherming wordt beschermd. Vanuit het perspectief van het bedrijfsleven kan bijvoorbeeld gedacht worden aan het toesturen van ongewenste commerciële communicatie en gepersonaliseerde reclame.

Categorisering van horizontale privacyschendingen

Op basis van de inbreukmakende handelingen en de belangen en waarden die in het geding zijn komen wij tot de volgende categorisering van horizontale privacyschendingen:

Horizontale privacyschendingen (burger-burger)		
Handelingen	*Verschijningsvormen*	*Aangetaste waarden / belangen*
Observeren	Heimelijk filmen, filmen in de publieke ruimte, afluisteren, spionage	Vertrouwelijkheid en controle, vertrouwen in intieme relaties, identiteit en emotionele ontlading, persoonlijke autonomie, (gevoel van) veiligheid, eer
Verzamelen en vastleggen	Heimelijk filmen, filmen in de publieke ruimte, afluisteren, spionage	Vertrouwelijkheid en controle, vertrouwen in intieme relaties, identiteit en emotionele ontlading, persoonlijke autonomie, (gevoel van) veiligheid, eer

Analyseren en beslissen	*Profiling* en (geautomatiseerde) besluitvorming	Vertrouwelijkheid en controle, eer en goede naam, persoonlijke autonomie
Creëren en delen	Belediging, smaad, laster, haatzaaien, bedreiging, afpersing, wraakporno, *sextortion*, *deepfakes*, *fake endorsement*, doen van niet gedane uitingen, *fake news*	Vertrouwelijkheid en controle, vertrouwen in intieme relaties, persoonlijke autonomie, identiteit en emotionele ontlading, eer en goede naam, (gevoel van) veiligheid,
Interacteren en communiceren	*Trolling*, belaging (*stalking*), cyberpesten	(gevoel van) veiligheid, persoonlijke autonomie, eer en goede naam

Horizontale privacyschendingen (burger-bedrijfsleven)		
Handelingen	*Verschijningsvormen*	*Aangetaste waarden / belangen*
Observeren	Monitoren surfgedrag, *Wifi tracking*	Vertrouwelijkheid en controle, persoonlijke autonomie
Verzamelen en vastleggen	Klantsystemen, vastleggen surfgedrag	Vertrouwelijkheid en controle, persoonlijke autonomie
Analyseren en beslissen	*Nudging*, *profiling*, geautomatiseerde besluitvorming	Vertrouwelijkheid en controle, persoonlijke autonomie, eer en goede naam,
Creëren en delen	Zwarte lijsten, delen / verkopen van gegevens	Vertrouwelijkheid en controle, persoonlijke autonomie, eer en goede naam
Interacteren en communiceren	Ongewenste commerciële communicatie	(Gevoel van) veiligheid, voorkomen van hinder.

De horizontale werking van het recht op privacy

Bij de totstandkoming van de klassieke grondrechten was de gedachte dat deze enkel ten opzichte van de overheid golden. De ratio hiervoor was dat burgers en private rechtspersonen min of meer gelijkwaardig waren en aldus onderling via het civiele recht eventuele aantastingen van hun rechten konden aanvechten. Met de tijd is deze opvatting echter veranderd. In zowel de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) als in de nationale rechtsorde van Nederland en de overige door ons onderzochte landen is de horizontale werking van grondrechten erkend. Rode draad hierbij is de erkenning van algemene persoonlijkheidsrechten die voortvloeien uit de menselijke waardigheid. Deze persoonlijkheidsrechten kunnen tegen eenieder worden ingeroepen.

In de door ons onderzochte landen is de erkenning van de horizontale werking van grondrechten op verschillende wijze geconstrueerd. Zo vloeit in Duitsland de horizontale werking van grondrechten voort

uit de grondwettelijk beschermde menselijke waardigheid. Het Duitse Constitutionele Hof oordeelde dat deze grondwettelijke bescherming tegen eenieder kon worden ingeroepen. In Polen is de horizontale werking van grondrechten vastgelegd in de grondwet. In het Verenigd Koninkrijk is de horizontale werking via de *Human Rights Act 1998* en de daarbij behorende jurisprudentie onderkend. Tenslotte is met name door de uitspraken van het EHRM ook in Zweden de horizontale werking van grondrechten geaccepteerd.

In Nederland heeft de Hoge Raad de horizontale werking van grondrechten ook geaccepteerd. De horizontale werking van grondrechten vloeit volgens de Hoge Raad voort uit de algemene persoonlijkheidsrechten die hun oorsprong hebben in de menselijke waardigheid.

De ontwikkelingen in het Verenigd Koninkrijk en Zweden tonen de invloed van het EVRM daar waar het gaat om de horizontale werking van grondrechten. Het EHRM construeert de horizontale werking van grondrechten allereerst via de positieve verplichting van verdragspartijen om grondrechten te beschermen. Een tweede wijze waarop het EHRM zorgt voor horizontale werking van grondrechten is door het afdwingen van verdragsconforme interpretatie door nationale rechters. Wanneer de nationale rechters onvoldoende acht slaan op de bescherming van de grondrechten van burgers (ook in horizontale verhoudingen) wordt door het EHRM aangenomen dat de staat tekortgeschoten is in het nakomen van haar verdragsrechtelijke verplichtingen.

We concluderen dat zowel op basis van ontwikkelingen in de nationale rechtsorde als door de werking van het EVRM, de horizontale werking van grondrechten geaccepteerd is in zowel Nederland als de door ons onderzochte landen. Polen en Duitsland kennen de meest expliciete erkenning van de horizontale werking van het recht op privacy. Of nadere codificatie van de horizontale werking van het recht op privacy in de Grondwet (naar Pools model) of de introductie van een zelfstandig recht op informationele zelfbeschikking (naar Duits model) noodzakelijk of zinvol is betwijfelen wij. Expliciete erkenning van de horizontale werking van grondrechten in de Nederlandse Grondwet lijkt primair symbolisch, omdat op het niveau van het EVRM de horizontale werking van grondrechten reeds wordt onderkend. Ditzelfde geldt voor een recht op informationele zelfbeschikking. Het recht op privacy is niet absoluut en wordt begrensd door andere rechten. Het introduceren van een recht op informationele zelfbeschikking is, in de woorden van de Commissie Franken, daarom niet veel meer dan een kwestie van “veel geven om daarna weer veel terug te nemen”. Daarnaast moet ook niet uit het oog worden verloren dat met de dwingende Europese wetgeving op het gebied van gegevensbescherming (de Algemene Verordening gegevensbescherming) de bandbreedte voor het invoeren van een nationaal recht op informationele zelfbeschikking überhaupt zeer beperkt is.

De bescherming van het recht op privacy in formele wetgeving

De grondrechtelijke bescherming van de horizontale privacy krijgt daadwerkelijk gestalte in lagere wetgeving. Hierbij kan gedacht worden aan het gegevensbeschermingsrecht, het civiele recht en het strafrecht.

Gegevensbeschermingsrecht
Zowel het recht op privacy als het recht op gegevensbescherming hebben een zeer brede reikwijdte. Bij beide rechten geldt dat ze in horizontale relaties kunnen botsen met andere (grond)rechten. In bedrijf-burger relaties gaat het dan bijvoorbeeld om een botsing met de vrijheid van onderneming en in burger-burger relaties om de vrijheid van meningsuiting. Een rechter zal bij een dergelijke botsing van geval tot geval beoordelen of een inperking van het recht op privacy of gegevensbescherming in dat geval legitiem is.

Het gegevensbeschermingsrecht, meer specifiek de Algemene Verordening gegevensbescherming (AVG) is in het bijzonder relevant in de relatie burger-bedrijfsleven. De AVG is niet van toepassing wanneer burgers persoonsgegevens verwerken voor puur huishoudelijke doeleinden. Wanneer de gegevens echter buiten de huishoudelijke kring komen (bijvoorbeeld door publicatie op internet), dan is de AVG wel van toepassing.

Als het gaat om het verwerken van bijzondere persoonsgegevens, waarmee gevoelige zaken over een persoon duidelijk worden, mag de verwerking in principe niet. Er is dan een uitzonderingsgrond nodig, zoals de uitdrukkelijke toestemming van de betrokkene. Als het gaat om het verwerken van 'gewone' persoonsgegevens kan het zijn dat een gerechtvaardigd belang van de verwerkingsverantwoordelijke het privacybelang van de betrokkene overstijgt. Daarvan kan sprake zijn bij het maken van camerabeelden in en om het huis vanwege veiligheidsredenen. In hoeverre dit ook opgaat in het geval van recreatieve doeleinden is niet eenduidig te zeggen en moet van geval tot geval worden beoordeeld. Voor het verwerken van persoonsgegevens met als doel het toebrengen van schade of nadeel aan de betrokkene zal vrijwel nimmer kunnen worden vertrouwd op deze verwerkingsgrond.

Wanneer de AVG van toepassing is, dan gelden naast de eis van het hebben van een legitiem doel voor de verwerking, tal van plichten voor de verwerkingsverantwoordelijke. Het gaat dan om andere beveiligingsplichten, informatieplichten, verantwoordingsplichten en het respecteren van de rechten van betrokkenen.

Omdat het gegevensbeschermingsrecht sterk geharmoniseerd is door de AVG hebben wij in de rechtsvergelijking geen noemenswaardige verschillen gevonden die voor het onderwerp van dit onderzoek relevant zijn.

Strafrecht
De rechtsvergelijking laat een redelijk uniform beeld zien daar waar het gaat om de strafrechtelijke sanctionering van horizontale privacyschendingen. In alle onderzochte landen zijn uitingsdelicten (smaad, laster), zedendelicten (voyeurisme, wraakporno, schennis van de eerbaarheid) en misdrijven gericht tegen de vrijheid (bedreiging, *stalking*) strafbaar gesteld. Op basis van de rechtsvergelijking lijken er ten opzichte van het buitenland geen grote hiaten te zijn in de strafrechtelijke normering van horizontale privacyschendingen in Nederland. Wel zijn er een aantal aspecten met betrekking tot de strafrechtelijke normering van horizontale privacyschendingen in het buitenland die interessant kunnen zijn voor de Nederlandse rechtspraktijk.

In vergelijking met de onderzochte landen kent Nederland allereerst ten opzichte van een aantal van de door ons onderzochte landen een beperktere strafbaarstelling voor het maken en verspreiden van gevoelige informatie. In Nederland is de strafbaarstelling primair beperkt tot het maken en verspreiden van beelden van een seksuele aard (artikel 139h Sr). Het vastleggen en verspreiden van beelden van bijvoorbeeld hulpbehoevenden, of het verspreiden van gegevens betreffende iemands gezondheidstoestand, zijn handelingen die niet zelfstandig strafbaar gesteld. Wel kan het verspreiden van dergelijke informatie onder omstandigheden onder het delict smaad worden gevat. Hiervoor is het evenwel noodzakelijk dat de eer of goede naam van het slachtoffer is aangetast. Mocht de informatie op illegale wijze zijn verkregen (bijvoorbeeld door het overnemen van gegevens of het heimelijk filmen van personen), dan biedt dat ook aanknopingspunten voor strafrechtelijke vervolging in Nederland.

In Nederland is in tegenstelling tot Duitsland en Zweden het filmen van hulpbehoevenden niet zelfstandig strafbaar gesteld. Onder omstandigheden kan wel het nalaten van het bieden van hulp ten laste worden gelegd. Het moet dan wel gaan om een situatie waarbij de filmer daadwerkelijk hulp had kunnen verlenen en zich daar ook van bewust was. Dit lost daarmee niet het probleem op van omstanders die slachtoffers filmen, bijvoorbeeld als hulpverleners reeds ter plaatse zijn. Eventueel zou nog het delict van artikel 426bis Sr ten laste kunnen worden gelegd bij filmers die hinderlijk in de weg staan, maar daarvoor is het wel noodzakelijk dat de filmer anderen in de vrijheid van hun beweging belemmert. Een mogelijk negatief effect van de strafbaarstelling van het filmen van hulpbehoevenden (bijvoorbeeld bij verkeersongelukken) is dat het de opheldering van delicten kan bemoeilijken. Ook kunnen de beelden van omstanders een rol spelen in bijvoorbeeld aansprakelijkheids- en verzekeringskwesties. Bij een eventuele strafbaarstelling zou hiermee rekening moeten worden gehouden.

De strafbaarstelling van aanstootgevend gedrag en obsceniteit is cultureel bepaald. Doel is enerzijds de bescherming van de goede zeden binnen de maatschappij en anderzijds het voorkomen dat individuen geschokt worden of aanstoot nemen aan bepaalde gedragingen of informatie. Het Verenigd Koninkrijk en Polen kennen regelingen waarmee de overheid kan optreden tegen de verspreiding van aanstootgevende of obscene beelden, in het bijzonder wanneer deze bedoeld zijn om irritatie of onnodige stress op te wekken. In Nederland kennen wij weliswaar de schennis van de eerbaarheid door het toezenden van aanstootgevend materiaal (artikel 240 Sr), maar deze strafbaarstelling is beperkt tot het toezenden van pornografisch materiaal. In zowel Polen als het Verenigd Koninkrijk zijn er door het ontbreken van deze afbakening in beginsel meer mogelijkheden om op te treden tegen grensoverschrijdend gedrag online. Ernstige vormen van *pranking* of *trolling* zouden bijvoorbeeld binnen de delictsomschrijving kunnen vallen als het publiek daar voldoende aanstoot aan neemt. In Nederland is dit type grensoverschrijdend gedrag niet zelfstandig strafbaar gesteld. Afhankelijk van de omstandigheden van het geval kunnen dit soort gedragingen wel strafbaar zijn, bijvoorbeeld wanneer er sprake van mishandeling of vernieling. Of bredere strafbaarstellingen van grensoverschrijdend gedrag in Nederland wenselijk zijn, is een politieke keuze. Een bredere strafbaarstelling voor het openbaar maken of toezenden van informatie biedt weliswaar meer mogelijkheden om horizontale privacyschendingen tegen te gaan, maar daar staat tegenover dat de vrijheid van meningsuiting onder druk kan komen te staan wanneer er geen heldere afbakening is van het

type materiaal dat als obsceen, aanstootgevend, kwetsend of anderszins schadelijk wordt gezien. Ook bestaat er het gevaar van willekeur in de toepassing.

Verder valt bij de strafbaarstelling in de onderzochte landen op dat veel uitingsdelicten geen klachtdelicten zijn zoals in Nederland. Dit biedt de overheid meer mogelijkheden om autonoom normstellend op te treden. Ook hier is het de vraag of dit wenselijk is met het oog op de vrijheid van meningsuiting, omdat het de overheid meer ruimte geeft om sturend op te treden tegen (lichte) schendingen van de privacy. Tenslotte zijn in een aantal landen de straffen voor uitingsdelicten hoger dan in Nederland.

Samenvattend kunnen wij stellen dat horizontale privacyschendingen vanuit het strafrecht effectief aangepakt kunnen worden. Vraag is wel in hoeverre de bestaande bescherming ook daadwerkelijk in de praktijk geeffectueerd wordt. Deze vraag vormde niet het voorwerp van ons onderzoek maar is uiteraard wel van belang bij de beoordeling hoe goed de strafrechtelijke bescherming van de horizontale privacy in de praktijk is.

Consumentenrecht, administratief recht en mededingingswetgeving
Het consumentenrecht richt zich op de bescherming van consumenten, die als zwakkere partij worden gezien. Zo worden burgers in deze 'diagonale verhoudingen' beschermd tegen bedrijven die misbruik maken van hun macht of misleidend te werk gaan. Het mededingingsrecht sluit hierbij aan. Via het mededingingsrecht kunnen grote internetbedrijven als Facebook, Microsoft en Google aangepakt worden voor misbruik van hun monopoliepositie. Niet voor niets heeft onder meer de European Data Protection Supervisor gewezen op het feit dat in *Big Data* processen vaak sprake is van een samenloop van gegevensbeschermings-, consumentenbeschermings- en mededingingsrecht. Daarom heeft het opgeroepen tot meer samenwerking tussen de toezichthouders die toezien op de naleving van deze wetten: in Nederland zijn dat de Autoriteit Persoonsgegevens en de Autoriteit Consument en Markt.

De vraag daarbij is wel in hoeverre het realistisch en wenselijk is dat deze drie rechtsgebieden in de relatie burger-burger een rol gaan spelen; eerder lijkt het voor de hand te liggen dat ze diagonale relaties (de relatie tussen burgers en grote bedrijven) inkaderen. Het is namelijk vaak ondoenlijk en onwenselijk als overheidsinstanties of –functionarissen gaan controleren op alledaags gebruik van alledaagse producten in horizontale verhoudingen waarmee evenwel de onderlinge privacy geschonden kan worden, zoals *smartphones*, *drones*, *IoT devices* en andere soft- en hardware.

Civiel recht
Het civiel recht kent in zowel Nederland als de door ons onderzochte landen veel mogelijkheden om op te treden tegen horizontale privacyschendingen. De belangrijkste actie is die uit onrechtmatige daad. Wanneer het slachtoffer van een horizontale privacyschending schade lijdt, dan moet deze vergoed worden door de verweerder. Dit geldt niet alleen voor vermogensschade, maar op grond van artikel 6:106 BW en de daarbij behorende jurisprudentie, ook voor reputatieschade en immateriële schade. De enkele schending van het recht op privacy zal overigens niet direct een verplichting tot schadevergoeding opleveren, het moet of gaan om een ernstige schending waardoor schade voor het individu aannemelijk is, dan wel moet de eiser daadwerkelijk kunnen aantonen dat er sprake is van schade.

Wel kent het civielrecht met betrekking tot het beschermen van de horizontale privacy twee beperkingen.

Allereerst is het civiel recht grotendeels reactief. Hoewel op grond van het civiel recht wel pro-actief kan worden opgetreden tegen horizontale privacyschendingen, bijvoorbeeld door het verbieden van een voorgenomen onrechtmatige perspublicaties, heeft dit in de relatie burger-burger weinig waarde, omdat vaak op voorhand niet duidelijk is dat een burger een privacyschending gaat plegen. Dan resteert de actie uit onrechtmatige daad om de schending te beëindigen en eventuele schade te vergoeden.

De tweede beperking ligt in de mogelijkheden voor de benadeelde om daadwerkelijk zijn of haar recht te halen. Procedures voor een rechter zijn kostbaar en risicovol. Het feit dat op internet veel horizontale privacyschendingen anoniem of pseudoniem worden gedaan maakt zelfstandig optreden door burgers nog lastiger. Het probleem van een moeilijke of kostbare rechtsgang wordt deels geadresseerd door de mogelijkheid tot het voeren van collectieve procedures, maar deze optie staat maar voor een beperkte categorie privacyschendingen open.

Tenslotte moet nog worden opgemerkt dat een gang naar de civiele rechter (of het doen van aangifte) voor benadeelden niet altijd een optie is. Zeker in gevoelige zaken, zoals bijvoorbeeld de verspreiding van naaktbeelden, zijn de confrontatie met de dader en de openbaarheid van de procedure soms redenen voor het slachtoffer om niet te procederen. Een procedure zorgt daarmee als het ware voor een voortduring of verergering van de privacyschending. Afgeschermde dan wel niet-openbare procedures zouden dit probleem kunnen adresseren. Hierbij speelt natuurlijk wel het negatieve effect op de openbaarheid van de rechtspraak.

De rol van producenten, distributeurs en internettussenpersonen

Aansprakelijkheid van producenten en distributeurs
In Nederland en de meeste landen uit de rechtsvergelijking zijn wij geen bepalingen tegengekomen die bepaalde type producten (afluisterapparatuur, *spycams*, *stalkerware*) op voorhand verbieden of specifieke regels stellen voor de verkoop ervan. Alleen Duitsland heeft een (beperkt) verbod op het gebruik van apparatuur die gebruikt kan worden om mensen af te luisteren. Ook kan er op grond van de regels voor productaansprakelijkheid niet worden opgetreden tegen producenten van hardware en software die overduidelijk bestemd is voor het plegen van horizontale privacyschendingen.

Aansprakelijkheid van internettussenpersonen
Met betrekking tot de rol van internettussenpersonen bij de bestrijding van horizontale privacyschendingen is de vraag van belang in hoeverre zij aansprakelijk zijn voor het gedrag van gebruikers dan wel in hoeverre zij een plicht hebben om schendingen te voorkomen. Op grond van de huidige Europese regeling (de Richtlijn elektronische handel), is het uitgangspunt dat internettussenpersonen niet aansprakelijk zijn wanneer zij niet weten of behoren te weten dat er sprake is van een onrechtmatige gedraging en wanneer die wetenschap er wel is prompt handelen om de betreffende informatie te verwijderen.

Vooralsnog lijkt het erop dat op basis van het Unierecht partijen als Facebook en Twitter zich kunnen beroepen op de vrijwaringen voor de aansprakelijkheid ex. artikel 14 Reh, daar waar het gaat om de informatie die gebruikers zelf posten. Ook zijn deze internetplatformen op grond van artikel 15 Reh niet gehouden zijn om pro-actief hun platformen te monitoren op schadelijke content. Wel kunnen zij verplicht worden door nationale rechters om maatregelen te implementeren om toekomstige inbreuken te voorkomen, maar dan is het kwaad reeds geschied. Het is hierbij ook de vraag of dit het vraagstuk van horizontale privacyschendingen oplost, omdat de maatregel moet zien op het verwijderen van gelijke of gelijksoortige content als in het geval dat voor de rechter is gekomen. Dit betekent dat voor elke horizontale privacyschending een gang naar de rechter noodzakelijk is.

Om internetplatformen te stimuleren om meer actie te ondernemen kan gedacht worden aan de introductie van een *good samaritan clause* zoals voorgesteld in *Mededeling inzake de bestrijding van illegale content online*. Een mogelijk schadelijk neveneffect van een dergelijke clausule is wel dat internetplatformen meer macht en controle over de inhoud van hun platform krijgen. Zij krijgen immers meer 'redactionele vrijheid' zonder dat daar een bijbehorende aansprakelijkheid voor in de plaats komt. Mocht er voor een *good samaritan clause* worden gekozen is het daarom zaak deze goed af te bakenen.

Een verdergaande stap is de introductie van een pro-actieve zorgplicht. Het EHRM heeft in *Delfi* het nemen van pro-actieve maatregelen niet uitgesloten, maar dit was wel in de context van een ander type internetdienst (een berichtenforum behorende bij een nieuwssite). In Europa wordt gewerkt aan een wijziging van het aansprakelijkheidsregime voor internettussenpersonen via de *Digital Services Act*. De verwachting is dat er een 'zorgplicht' voor internetplatformen komt. Wat deze zorgplicht behelst is echter nog niet duidelijk.

Wat bij de introductie van een eventuele zorgplicht problematisch is, is dat bij horizontale privacyschendingen, in tegenstelling tot auteursrechtelijk beschermde werken, veelal niet eenvoudig kan worden vastgesteld wanneer er sprake is van een inbreuk. Uitingen en het effect daarvan op de privacy van een betrokkene zijn sterk contextgebonden. Dit maakt het voor de tussenpersoon moeilijk om te beoordelen of er sprake is van een onrechtmatige uiting, in het bijzonder wanneer dat op grote schaal en dus geautomatiseerd moet gebeuren. Dit kan ertoe leiden dat internetplatformen liever ruime parameters kiezen om aansprakelijkheid te vermijden. Dit heeft een negatief effect op de vrijheid van meningsuiting.

Daar waar het gaat om een strengere aanpak van online illegale content lijkt Duitsland de strengste aanpak te kiezen met de *Netzwerkdurchsetzungsgesetz*. Ook Zweden heeft met de interpretatie van de oude BBS wetgeving juridische mogelijkheden om internetplatformen aansprakelijk te houden voor strafbaar gestelde schendingen van de horizontale privacy. Gesteld kan worden dat juridische 'stok achter de deur' om op internetplatformen snel en effectief op te laten treden tegen schendingen daarmee in Zweden en Duitsland groter is dan in Nederland. Wel moet het dan gaan om strafbare horizontale privacyschendingen. Naast het nemen van maatregelen door de internetplatformen zelf (verwijderen, blokkeren, filteren), kunnen ook gebruikers actie ondernemen tegen schendingen van hun privacy. Het gaat dan enerzijds om de uitoefening van de rechten uit de AVG (in het bijzonder het recht op verwijdering ex. artikel 17 AVG) en

anderzijds de mogelijkheden die het Burgerlijk Wetboek biedt (bijvoorbeeld een actie uit onrechtmatige daad).

Problematisch bij de uitoefening van deze rechten is dat de benadeelde zich in eerste instantie moet richten tot de internetplatformen en niet tot de achterliggende gebruiker die daadwerkelijk de schending heeft gepleegd. Met name daar waar het gaat om het krijgen van schadevergoeding maakt dit de drempel voor benadeelden om actie te ondernemen hoger, omdat zij eerst een procedure tegen het platform moet doorlopen (bijvoorbeeld om gebruikersgegevens te achterhalen) en daarna pas de procedure tegen de daadwerkelijke schender.

Overige mechanismen

Naast wet- en regelgeving zijn er ook andere mechanismen die gericht zijn op het reguleren van privacy in horizontale verhoudingen. Het gaat om zelfregulering, voorlichting en onderwijs.

Zelfregulering

Naast initiatieven in kleinere sociale verbanden waar wij als onderzoekers minder zicht op hebben, lijkt zelfregulering met name relevant te zijn bij het online delen van content. Zelfregulerende initiatieven van producenten en distributeur van hardware en software die gebruikt kunnen worden voor horizontale privacyschendingen (*spycams*, *stalkerware*) hebben wij niet kunnen vinden.

Zelfregulerende initiatieven om privacy in horizontale verhoudingen te beschermen zien wij met name in de context van online dienstverlening. Het gaat daarbij om internetplatformen en andere dienstverleners die zelfstandig, of in publiek-privaat verband werken aan de regulering van online content. Publiek-private initiatieven om online content te reguleren zien primair op het tegengaan van illegale content zoals beelden van kindermisbruik, racistische of xenofobische content (haatzaaien) en terroristische content (verheerlijken of aanzetten tot terrorisme).[1] Overige schendingen van de horizontale privacy (zoals bijvoorbeeld het geval kan zijn bij belediging of wraakporno) worden door internetdienstverleners hoofdzakelijk zelf gereguleerd via *community standards* en *abuse policies*. Hoewel zelfregulering via gebruiksvoorwaarden een krachtig instrument is om horizontale privacyschendingen tegen te gaan, zijn er ook zorgen over mogelijke ongewenste neveneffecten. Zo waarschuwde de Speciale VN Rapporteur voor de vrijheid van meningsuiting dat de internetplatformen te zelfstandig kunnen reguleren op basis van hun community standards.

Onderwijs en voorlichting

Op het gebied van onderwijs en voorlichting is er een redelijk uniform beeld als we kijken naar de door ons onderzochte landen. Dit valt deels te verklaren vanuit het feit dat veel voorlichting, meer specifiek de voorlichting gericht op kinderen, Europees gecoördineerd wordt. Hierdoor kunnen landen succesvolle campagnes en leertrajecten van elkaar overnemen.

[1] Ook op het gebied van nepnieuws (fake news) en desinformatie zijn er zelfregulerende initiatieven, maar omdat deze voor het onderwerp van deze rapportage minder van belang zijn, hebben wij deze buiten beschouwing gelaten.

Overzicht normering en rechtsbescherming horizontale privacy

Op basis van ons onderzoek komen we tot het volgende overzicht van inbreuken en de bijbehorende normering en rechtsbescherming:

Normering en rechtsbescherming privacy in horizontale verhoudingen						
Type inbreuk	**Voorbeelden**	**Normering en bescherming**				
		Wet- en regelgeving				Overige mechanismen (zelfregulering)
		Strafrecht	Gegevensbescherming	Administratief recht, mededinging, consumentenrecht	Civiel recht	
Observeren, verzamelen en vastleggen	Voyeurisme, (heimelijk) cameratoezicht, afluisteren, gebruik *spy-* en *stalkerware*, heling gegevens, filmen slachtoffers	Computervredebreuk (138ab Sr), overname gegevens (138c Sr), afuisteren (139c Sr), heimelijk opnemen gespreken (139a, b Sr), heimelijk cameratoezicht (139f Sr), bezitten / verwerven gegevens (139e, g Sr), belaging (285 Sr)	Onrechtmatige verwerking, recht op verwijdering (17 AVG)	Administratief recht (APV), consumenten-bescherming, productveiligheid, oneerlijke handelspraktijen	Onrechtmatige daad, schending portretrecht	*Naming and shaming*
Analyseren en beslissen	*Profiling* en geautomatiseerde besluitvorming		Onrechtmatige verwerking, recht op verwijdering (17 AVG), verbod geautomatiseerde besluitvorming (22 AVG)	Consumenten-bescherming	Onrechtmatige daad	
Creëren en delen	Belediging, *deepfakes*, valse advertenties. Toeschrijven van uitspraken aan een persoon, misbruik identiteit, wraakporno	Groepsbelediging, haatzaaien (137c en d Sr), belediging (266 Sr), smaad (261 Sr), laster (262 Sr), wraakporno (139h Sr),	Onrechtmatige verwerking, correctierecht (16 AVG), verwijderingsrecht (art. 17 AVG)	-	Onrechtmatige daad, rectificatierecht , portretrecht.	Overtreding gebruiksvoorwaarden platformen, *naming and shaming*

Interacteren en communiceren	Stalking, bedreiging, *sextortion*, cyberpesten, (verder: belediging, smaad, laster)	285 Sr, bedreiging (317 Sr), wraakporno (139h Sr), oplichting (225 Sr, 326 Sr)	Onrechtmatige verwerking, Correctierecht (art. 16 AVG), verwijderingsrecht (art. 17 AVG)	-	Onrechtmatige daad	Overtreding gebruiksvoorwaarden platformen, *naming and shaming*.

Inpassen van buitenlandse rechtsfiguren in de Nederlandse rechtsorde

Op basis van ons onderzoek concluderen wij dat de horizontale privacy in de door ons onderzochte landen op een min of meer gelijke wijze is gereguleerd. Dit betekent dat er relatief weinig 'te halen' valt in het buitenland. Rechtsfiguren uit het buitenland die kunnen bijdragen aan een betere bescherming van de horizontale privacy liggen primair in het strafrecht en de regels betreffende de aansprakelijkheid van internetplatformen.

Een eerste strafrechtelijke bepaling waarnaar gekeken kan worden is een bredere strafbaarstelling voor het openbaarmaken en verspreiden van aanstootgevende of obscene content zoals dit in Polen en het Verenigd Koninkrijk is strafbaar gesteld. Het voordeel van een dergelijke bepaling is dat het veel flexibiliteit biedt om autonoom normstellend en handhavend op te treden. Een groot risico bij het invoeren van een dergelijke bepaling is de rechtsonzekerheid. Wanneer er geen heldere afbakening bestaat voor het type materiaal dat als obsceen, aanstootgevend, kwetsend of anderszins als schadelijk wordt gezien, ligt het gevaar van censuur en willekeur op de loer.

Een tweede strafrechtelijke bepaling die in aanmerking kan komen voor transplantatie in de Nederlandse strafwet is het filmen van hulpbehoevende personen. Het invoeren van een verbod op het filmen van hulpbehoevenden heeft potentieel een effect op de vrijheid van meningsuiting, maar wanneer de bepaling voldoende ruimte biedt voor bijvoorbeeld uitzonderingen in het kader van de pers, kan waarschijnlijk een goede balans tussen het recht op privacy en het recht op vrijheid van meningsuiting worden gevonden. Een ander relevant aspect is dat beelden van omstanders ook kunnen bijdragen aan de opheldering van een misdrijf of het beter vast kunnen stellen van de toedracht van een ongeluk. Hier moet bij een eventuele strafbaarstelling rekening mee worden gehouden.

Wanneer de wetgever besluit om strengere eisen te stellen aan internetplatformen, dan kan de Duitse Netwerkhandhavingswet een voorbeeld bieden. Hoewel de effecten van de wet (zowel positief als negatief) nog niet vaststaan, kan wel worden gesteld dat dergelijke bepalingen de vrijheid van meningsuiting aan kunnen tasten. Maatregelen gericht aan het adres van de internetplatformen kunnen naast de vrijheid van meningsuiting ook de vrijheid van ondernemerschap aantasten en mogelijk het economische vestigingsklimaat en de innovatie in Nederland beïnvloeden. Mocht de wetgever m nadere regels met betrekking tot de aansprakelijkheid van internettussenpersonen overwegen, dan is het van belang dat deze goed aansluiten op het Europese regime dat momenteel herzien wordt.

Rechtsfiguren niet ontleend aan het buitenland

Naast het inpassen van buitenlandse bepalingen kunnen ook nog enkele voorstellen worden gedaan die niet rechtstreeks uit de rechtsvergelijking naar voren komen, maar voortkomen uit de eigen analyse van de Nederlandse en buitenlandse rechtsbescherming.

Een eerste optie is het verkennen van strengere eisen aan de verkoop van producten en diensten die hoofdzakelijk gemaakt zijn om inbreuk te maken op de persoonlijke levenssfeer. Hierbij kan in het bijzonder worden gedacht aan *spycams*, peilbakens en *stalkerware*. Zo kunnen bijvoorbeeld beperkingen worden gesteld aan de verkoop van dergelijke producten aan particulieren, aanvullende eisen aan de informatievoorziening of een vergunningsstelsel voor verkopers en/of gebruikers. Dergelijke maatregelen gaan minder ver dan een volledig verbod.

Ten tweede zou kunnen worden onderzocht in hoeverre technische eisen kunnen worden gesteld om bepaalde opnames onmogelijk te maken (of in ieder geval veel moeilijker). Hierbij kunnen we denken aan *geo-fencing* ten aanzien van *no-fly zones* voor drones, of het automatisch *blurren* van gezichten bij het gebruik van camera's in specifieke ruimten. Daarnaast kan gekeken worden in hoeverre er technische eisen kunnen worden gesteld aan producten om de heimelijkheid van opnameapparatuur te verkleinen. Hierbij kan worden gedacht aan het verplicht afgeven van een geluidssignaal of lichtsignaal als producten opnames starten of maken. Met de *privacy by design* eis uit artikel 25 AVG bestaat er al deels een wettelijke basis om dergelijke maatregelen af te dwingen.

Toekomstige regulering van horizontale privacyschendingen

Als het aankomt op juridische maatregelen om de horizontale privacy beter te beschermen dan zijn er grofweg twee opties: 1) maatregelen nemen die gericht zijn op het terugdringen van de mogelijkheden om de privacy te schenden (*ex ante*, preventieve maatregelen), en 2) maatregelen die zijn gericht op het beëindigen van privacyschendingen en het compenseren van de slachtoffers (*ex post*, reactieve maatregelen).

Bij de eerste categorie maatregelen kan gedacht worden aan het verbieden van bepaalde producten of diensten, of het verbinden van vergunningseisen aan de verkoop of koop van dergelijke producten zoals hierboven beschreven. Een nadeel van deze aanpak is dat de meeste producten (denk aan een *smartphone* of *drone*) zowel voor legitieme als illegale doelen kunnen worden ingezet. Op voorhand is het daarmee problematisch om bepaalde producten of diensten te verbieden of de verkoop en het gebruik ervan nader te reguleren.

Een voordeel van *ex post* regulering is dat de legale toepassingen en het rechtmatige gebruik van technologie niet op voorhand worden verboden. Het nadeel is echter dat de toepassingen zo wijdverbreid zijn dat het vrijwel onmogelijk is om alle inzet van technologie in horizontale verhoudingen te toetsen op legitimiteit (ofwel door burgers zelf, door burgerrechtenorganisaties of door overheidsinstanties) en dat het leed al is geschied als er juridische stappen volgen. Hoogstens kan een burger nog schade verhalen, maar ook dat zal vaak lastig blijken, omdat de dader van een schending niet altijd te achterhalen is, omdat er bewijsrechtelijke obstakels bestaan, omdat de schade niet kwantificeerbaar of eenvoudig te duiden is,

of omdat de burger simpelweg niet nog meer aandacht wil vestigen op datgene wat met de privacyinbreuk is onthuld.

Een tussenvorm is om ons niet zozeer te richten op voorkomen van het begaan van een privacyinbreuk, als wel op het verder verspreiden van onrechtmatig verkregen informatie over andere burgers. Hierbij spelen met name de internetdiensten en -platformen een belangrijke rol. De vraag is in hoeverre deze platformen een pro-actieve rol spelen of moeten spelen bij het tegengaan van horizontale privacyschendingen. Er is weliswaar een algemene zorgplicht, maar hoever die reikt in de digitale context is niet op alle punten duidelijk.

Rechtsbescherming in de praktijk

Ook al wordt de horizontale werking van grondrechten erkend, het primaire uitgangspunt blijft dat in horizontale relaties partijen min of meer gelijkwaardig zijn en daarom onderling eventuele geschillen moeten oplossen. Hoewel een toets van de effectiviteit van privacybeschermende maatregelen niet de opdracht voor dit onderzoek vormde, kunnen wij op basis van ons onderzoek in ieder geval wel vraagtekens plaatsen bij de daadwerkelijke rechtsbescherming voor burgers. Enerzijds is het voor burgers moeilijk om op te treden tegen privacyschendingen, anderzijds is de capaciteit van de overheid (politie, justitie, toezichthouders) om de gestelde normen te handhaven ook beperkt. Eventuele versterking van het recht op privacy in wet- en regelgeving kan daarom nooit los worden gezien van de daadwerkelijke mogelijkheden van burgers en de capaciteit om te handhaven bij de overheid.

Daarnaast is het van belang in te zetten op de ontwikkeling van sociale en maatschappelijke normen voor de digitale context. In tegenstelling tot de fysieke wereld zijn de normen in de digitale wereld nog minder vastomlijnd. Ook speelt de relatieve afwezigheid van gezaghebbende instituties een rol in het ontstaan en voortduren van privacyschendingen. Voorlichting en zelfregulering kunnen helpen bij het vormen en handhaven van normen en waarden op plaatsen waar deze zich nog niet hebben ‘gezet’ en de overheid een minder sterke aanwezigheid heeft.

Een probleem dat in de digitale context speelt is dat maatschappelijke en sociale normen zich maar traag ontwikkelen. Het duurt vaak een decennium voordat dergelijke algemeen geaccepteerde standaarden zich hebben bestendigd. Voor niet-digitale ontwikkelingen zijn dergelijke normen vaak de meest adequate vorm van normering, omdat ze breed gedragen worden, geïnternaliseerd raken en mensen elkaar daar zonder probleem op kunnen aanspraken. In de digitale context komen dergelijke normen echter vaak te laat; als een norm zich eenmaal heeft gematerialiseerd, dan staat is er vaak alweer een nieuwe toepassing, techniek of dienst. Overheden en/of maatschappelijke organisaties kunnen een belangrijke rol spelen bij de ontwikkeling en acceptatie van nieuwe sociale en maatschappelijke normen die direct inspelen op nieuwe technologische ontwikkelingen en toepassingen.

Tenslotte kunnen wij stellen dat gezien de snelle technologische ontwikkelingen en de maatschappelijke reacties daarop, de wetgever juist in de digitale omgeving moet investeren in mechanismen om technologische ontwikkelingen, nieuwe toepassingen en de mogelijke consequenties daarvan vroegtijdig te signaleren. Naast het versterken van bestaande instrumenten kan bijvoorbeeld een vaste

Kamercommissie ‘digitale toekomst’ bijdragen aan het vroegtijdig signaleren en analyseren van nieuwe horizontale privacyvraagstukken.

1 Summary

Fundamental rights, such as the right to privacy, are primarily aimed at the protection of citizens against the state. But citizens may also violate the fundamental rights of others. For that reason, it is imperative to assess the extent to which fundamental rights (more specifically, the right to privacy) provide protection in 'horizontal relationships'. The issue of horizontal privacy was raised in the '*initiatiefnota onderlinge privacy*'. The topic of privacy violations in horizontal relationships is aimed at violations committed in the context of (i) actions of citizens towards each other and (ii) the relationship between citizens and legal persons (companies, associations, etc.). The protection of horizontal privacy is differentiated from the protection of vertical privacy, which concerns the relationship a citizen has with the state.

This research addresses a problem statement that can be divided into three sub-statements:

- What lessons can be learned from the approach taken by other European countries with regards to the protection of horizontal privacy?
- To what extent can these solutions be applied in the context of the Netherlands?
- Are there any undesirable consequences or side-effects associated with the opportunities to provide effective protection to horizontal privacy in the Netherlands?

The countries that are involved in the legal comparative analysis are: Germany, Poland, Sweden and the United Kingdom.

To address the problem statement, the following questions require answering:

- What is 'horizontal privacy' and how is it conceptualized in the Netherlands and the investigated European countries?
- What are the protected interests that may be affected by the impairment or violation of horizontal privacy?
- What are the current impairments to these interests?
- What are the various forms of prevention, enforcement and prosecution of violations currently used?
- What forms of cooperation exist between citizens, businesses and the government to combat the violations of horizontal privacy?
- How has the protection of horizontal privacy been designed in Germany, Poland, Sweden, and the United Kingdom?
- To what extent are protective measures from these countries useful in the context of the Netherlands?
- What are the potential negative effects of implementing these measures to better protect horizontal privacy?

The scope of this research is limited to 'digital' privacy violations. In this research, we focus on the (i) citizen-to-citizen relationship and (ii) the citizen-to-private legal person relationship (more specifically, the relationship between business and consumers/employees). However, the emphasis is placed on the discussion and analysis of privacy violations committed by citizens towards each other.

Violations of horizontal privacy

The privacy of citizens in horizontal relationships can be violated in any number of ways. This research makes a distinction between the actions leading to the invasion of privacy and the consequences that this can have for the individual and society as a whole (the values and interests that as a result are likely to be affected).

Actions that may affect the privacy of citizens that we have identified are: observation, the collection and registration of data, analysis and decision-making, creation, the sharing and publication of data and interaction and communication.

Observation
Privacy violation typically starts with the observation of individuals and their behavior. In the digital era, observation is not limited to literally 'watching' an individual (whether or not aided by technical resources) but also concerns the following of an individual on social media and monitoring an individual's behavior on the Internet.

Collection and registration
Observation often goes hand in hand with the actual collection and recording of (personal) data. Relevant examples are the recording of images or conversations on a mobile phone but also includes the registration of traffic data or the location of an individual.

Analysis and decision-making
Depending on the purpose, registered data can be analyzed. This is particularly relevant in the context of a citizen's relationship with businesses, because it is primarily these businesses that are engaged in the analysis of personal data and using this analysis to inform their (automated) decision-making. The underlying purpose is generally to gain insight into the behavior and desires of consumers.

Creation
In addition to the observation and registration, data concerning individuals can also be created. Good examples are the creation of photomontages, cartoons, and even memes. One could also think about creation and dissemination of statements and/or expressions and how they can be (mis)attributed to an individual.

Sharing and publication
Many violations of horizontal privacy concern the sharing of data (photos, text, videos, sounds). Data can be shared with a single person, a (relatively) limited group (a private WhatsApp groupchat), or a large and undefined group (Facebook, Instagram, or Twitter). The sharing of data exposes information relating to an individual (or exposes their identity) with the result that it (undesirably) becomes public.

Interaction and communication
Direct interaction and communication with a person can also affect his or her privacy. Through digital means of communication it becomes possible to contact an individual at any moment and to communicate with (or about) them. This kind of interaction can, depending on the nature and frequency of the communication,

result in the violation of that individual's privacy. Prominent examples are stalking, cyber-bullying, the communication of offensive insults or threats.

Values and interests

The right to privacy is a comprehensive right. Not only does the right to privacy have a broad scope, it also functions as an 'umbrella right' which serves to protect a wide range of values and interests. The current research has identified the relevant values and interests and divided them into the following groups: dignity and reputation, confidentiality and control, personal autonomy, the development of identity and emotional relief, maintaining (intimate) relationships, security, economic equality, and the prevention of nuisance.

Dignity and reputation

Dignity (or personal honor) and reputation form components of the right to privacy as set out in Article 8 of the European Convention on Human Rights. Honor and dignity refer to the value one has in his or her own eyes. Reputation concerns the value that one has in the eyes of others.

Confidentiality and control

A crucial element of the right to privacy is the possibility to restrict and exclude the access of others to one's private life (which includes information and communication). This control of private life enables an individual to temporarily withdraw from social interaction and also enables them to selectively share information and aspects of their personality. Confidentiality and control play an important role in the relationship between individuals and legal persons. For example, when companies collect personal data relating to individuals, these individuals lose control of their information.

Personal autonomy

Privacy is an important requirement for the preservation of personal autonomy. As others gain more knowledge about an individual (his or her interests, weaknesses, preferences, habits, contacts, *et cetera*), it becomes easier to exercise power over this individual (or manipulate them).

Development of own identity and emotional relief

A more specific element of the personal autonomy is the possibility for an individual to develop their own identity, free from the pressure and influence of others. The right to privacy creates a space to experiment with a personal identity and (temporarily) escape the pressure of societally acceptable or expected behavior.

Maintaining (intimate) relationships

Confidentiality is a condition for social relationships. For example, friendships are in large part formed by the exclusive transfer of information.

Another aspect of the right to privacy that affects relationships is the so-called *associative privacy*. Associative privacy concerns the relationships and contacts that individuals maintain. When these contacts are made public, especially without providing the necessary context, maintaining these contacts in the future is made difficult.

Security
The most extreme cases of violations of horizontal privacy can also create a threat to the safety of the victim or their sense of security. Examples are the communication of communicating offensive insults, threats, harassment (stalking) and cyber-bullying.

Economic equality
Where it concerns the relationship between a (potential) client and a business, the economic position of the client is particularly susceptible to privacy violations. Information asymmetry provides businesses with a dominant position in comparison to the consumer. This position can, among other things, be exploited in the form of price discrimination or *nudging* clients towards certain groups of products.

The prevention of nuisance
The prevention of nuisance is also an interest protected by the right to privacy and data protection. From the perspective of the commercial industry, relevant examples include the sending of unsolicited commercial communications and personalized advertising.

Categorizing horizontal privacy violations
Set out below is a categorization of horizontal privacy violations, determined on the basis of (i) actions with potentially violating effects and (ii) the aforementioned interests and values that are at stake.

Horizontal privacy violations (citizen-to-citizen)		
Actions	*Manifestations*	*Affected values / interests*
Observation	Covert observation, filming in the public space, eavesdropping, espionage	Confidentiality and control, trust in intimate relations, identity and emotional release, personal autonomy, (sense of) security, dignity
Collection and registration	Covert observation, filming in the public space, eavesdropping, espionage	Confidentiality and control, trust in intimate relations, identity and emotional release, personal autonomy, (sense of) security, dignity
Analysis and decision-making	Profiling and automated decision-making	Confidentiality and control, dignity and reputation, personal autonomy
Creation and sharing	Libel, defamation, slander, hate speech, threats, extortion, revenge porn, sextortion, deep fakes, fake endorsements, fake news.	Confidentiality and control, trust in intimate relations, identity and emotional release, personal autonomy, (sense of) security, dignity and reputation
Interaction and communication	*Trolling*, harassement (stalking), cyberbullying	personal autonomy, (sense of) security, dignity and reputation

Horizontal privacy violations (citizen-to-business)		
Actions	*Manifestations*	*Affected values / interests*
Observation	Monitoring online behaviour, Wifi tracking	Confidentiality and control, personal autonomy
Collection and registration	Customer relation management, registration of consumer behaviour	Confidentiality and control, personal autonomy
Analysis and decision-making	*Nudging*, *profiling*, automated decision-making	Confidentiality and control, personal autonomy, dignity and reputation
Creation and sharing	Selling personal data, black / whitelisting	Confidentiality and control, personal autonomy, dignity and reputation
Interaction and communication	Unsolicited (commercial) emails	Sense of security, avoiding nuisance

The horizontal application of the right to privacy

The intention with the creation of the classical fundamental rights was that these were only applicable with regards to the state. The underlying rationale was that citizens and private legal persons were more or less equal and could challenge any infringement of their rights caused by the other through civil law. This view has changed with the passage of time. The horizontal application of fundamental rights is recognized in the jurisprudence of the European Court of Human Rights (ECtHR), the national legal order of the Netherlands, and the legal orders of the European countries investigated for this research. The common thread is that recognizing the general rights relating to personality derives from human dignity. These rights relating to personality can be invoked against anybody.

In the European countries investigated for our research, the recognition of the horizontal application of fundamental rights finds different constructions. In Germany, the horizontal application of fundamental rights is derived from the constitutional protection of human dignity. The German Constitutional Court found that these constitutional protections could be invoked against anybody. In Poland, the horizontal application of fundamental rights is enshrined in its constitution. In the United Kingdom, the horizontal application is recognized through the *Human Rights Act 1998* and the associated jurisprudence. In Sweden, the judgments of the ECtHR have created the acceptance of the horizontal application of fundamental rights.

The Supreme Court of the Netherlands has also accepted the horizontal application of fundamental rights. According to the Court, the horizontal application of these rights is derived from the general rights relating to personality which find their origin in the concept of human dignity.

The development in the United Kingdom and Sweden shows the influence of the European Convention on Human Rights (ECHR) and the ECtHR concerning the horizontal application of fundamental rights. The ECtHR's construction of the horizontal application of fundamental rights begins with the positive obligation of Contracting Parties to protect fundamental rights. The second way the ECtHR ensures the horizontal application of fundamental rights is through the enforcement of treaty-compliant interpretation by national courts. Where national courts pay insufficient attention to the protection of the fundamental rights of citizens (including in horizontal relationships), the ECtHR will find that the state has failed to fulfill its Treaty obligations.

We conclude that on the basis of both developments in the national legal order and the operation of the ECHR, the horizontal application of fundamental rights has been accepted both in the Netherlands and the European countries in our analysis. Poland and Germany have the most explicit recognition of the horizontal application of the right to privacy. We doubt whether further constitutional codification of the horizontal application of the right to privacy (based on the Polish model) or the introduction of an independent right to informational self-determination (based on the German model) is necessary or useful. Explicit recognition of the horizontal application of fundamental rights in the Dutch Constitution would appear to primarily be symbolic because of the already present recognition at the level of the ECtHR. The same applies to a right to informational self-determination. The right to privacy is not absolute and can be restricted by other rights. Introducing a right to informational self-determination is therefore, in the words of the Franken Commission, little more than a question of 'giving a lot and then taking a lot back'. In addition, it should also be borne in mind that, with the binding European data protection legislation (the General Data Protection Regulation), the room for introducing a national right to informational self-determination is very limited.

The protection of the right to privacy in formal legislation

The constitutional protection of horizontal privacy is given actual shape in subordinate legislation. Examples are data protection law, civil law, and criminal law.

Data protection law

Both the right to privacy and the right to data protection are broad in scope and may conflict with other (fundamental) rights in horizontal relationships. In the relationship between citizens and businesses, this concerns a conflict with the freedom of enterprise, and, in the horizontal relationship between citizens, it primarily concerns the freedom of expression. In the event of such a conflict, a judge will have to assess on a case-by-case basis whether such a restriction of the right to privacy is legitimate.

Data protection law, more specifically the General Data protection Regulation (GDPR), is particularly relevant in the relationship between citizens and commercial industry. The GDPR does not apply when citizens process personal data for purely domestic purposes. However, the GDPR does apply if the data is processed outside this personal sphere (e.g. through the publication on the Internet).

If it concerns the processing of special categories of personal data, through which sensitive matters about an individual are made clear, the processing is in principle not permitted, unless the individual concerned

has provided, for instance, explicit consent. If it concerns the processing of 'ordinary' categories of personal data, it may also concern a legitimate interest of the data controller that outweighs the interest of the data subject. This may be the case when camera images are made in and around the house for the purpose of home security. The extent to which this applies in the case of recreational purposes cannot be unequivocally stated and will have to be assessed on a case-by-case basis. It will hardly ever be possible to rely on this lawful basis for processing if the processing of personal data is done with the aim of causing damage to the data subject or placing them at a disadvantage.

Where the GDPR is applicable, there are a number of obligations for the data controller that go beyond having a legitimate purpose for processing. An important example is informing the data subject when personal data is processed for purposes beyond those for which they were originally collected. This disallows the covert processing of personal data for any other reason than the original purpose of collection. Another obligation is the taking of appropriate technical and organizational security measures.

The high degree of harmonization within the field of data protection law has left this research with an absence of any noteworthy differences that could be relevant for this research.

Criminal law
The legal comparison shows a reasonable uniformity when it comes to the criminal sanctioning of horizontal privacy violations. In all of the European countries analyzed for this research, crimes of expression (libel, slander), crimes of indecency (voyeurism, revenge pornography, violation of honor), and crimes against freedom (threats, extortion) are punishable. On the basis of the comparative law analysis, there appears to be no major discrepancies in the criminal law standards of horizontal violations of privacy in the Netherlands with respect to other countries. There are, however, a number of aspects with regards to standard setting of horizontal privacy violations in respect to criminal law that may be of interest to the Dutch legal practice.

To begin, the Netherlands has a more limited criminal liability for the creation and dissemination of sensitive information. In the Netherlands, the offense is primarily limited to the making and distribution of images of a sexual nature (Article 139h of the Criminal Code). The capturing and distribution of images of, for example, people in need of help, or distributing data concerning someone's state of health, are acts that are not independently punishable. However, under certain circumstances, the dissemination of such information can fall under the criminal definition of libel. However, a precondition is that the victim's honor or good name be tarnished. Where the information has been obtained illegally (e.g. by copying data or secretly filming individuals), it will offer a possibility for criminal prosecution in the Netherlands.

Unlike Germany and Sweden, the filming of individuals in need of help is not independently punishable in the Netherlands. Although under certain circumstances, the failure to provide assistance can lead to a criminal charge. This should concern a situation in which the individual filming could have provided assistance and was aware of this. This does not solve the problem of bystanders who film victims, where emergency services are already at the scene. It is possible to be charged with an offense of obstruction, under Article 426bis of the Criminal Code, although the individual filming would have to have obstructed others in their freedom of movement. A possible negative consequence of criminalizing the filming of

individuals in need of assistance (e.g. traffic accident victims) is that it may make it more difficult to clarify offenses. The captured images of bystanders may also play a role with regards to relevant liability and insurance issues. This should be taken into account in the context of potential criminalization.

The extent to which offensive behavior and obscenity is criminalized is in large part culturally determined. On one hand, the aim is to protect morality within society and, on the other hand, to prevent individuals from being shocked or offended by certain behavior or information. The United Kingdom and Poland have regulations in place that allow the government to take action against the dissemination of offensive or obscene images, especially when they are aimed at causing irritation or unnecessary stress. In the Netherlands, the sending of offensive material may violate the honor of an individual (Article 240 Sr), but its application is limited to the sending of pornographic material. In both Poland and the United Kingdom, the absence of this limitation means that there are more opportunities to take action against unacceptable online behavior. For example, serious forms of pranking or trolling could fall within the scope of the offense and its definition if the public is sufficiently offended. In the Netherlands, this type of behavior is not independently punishable. However, depending on the circumstances of the case, this type of behavior may be punishable, in particular when maltreatment or destruction is involved. Whether the unacceptable behavior should be subject to broader criminalization in the Netherlands is ultimately a political issue. Wider criminalization for the disclosure or dissemination of information does offer more possibilities to counter horizontal privacy violations. Although on the other hand, freedom of expression might be threatened if there is no clear definition of what is considered obscene, harmful, or otherwise hurtful. In addition, there is also a danger this broader criminalization might lead to arbitrary application.

Furthermore, in the European countries analyzed for this research, it is clear that many crimes of expression are not crimes conditional on a complaint like in the Netherlands. This offers the government more possibilities to act autonomously in setting standards. Even here, the question surrounding whether this is desirable with a view on safeguarding the freedom of expression, because it provides the government with more leeway to take direct action against (minor) violations of privacy. Finally, in a number of countries the penalties for crimes against expression crimes (e.g. libel and slander) are higher than in the Netherlands.

To summarize, we can state that violations of horizontal privacy from a criminal law perspective can be addressed effectively. Although, the question is to what extent the existing protection is actually enforced in practice. This question was not the subject of the current research but its importance is evident when assessing the effectiveness of the protection of horizontal privacy in the context of criminal law.

Consumer protection law, administrative law and competition law
Consumer protection law focuses on the protection of consumers, who are often regarded as the weaker party in their relationships with entities in the commercial industry. Citizens are protected in their diagonal relationships against service providers who abuse their power or act in a misleading or deceptive way. Competition law takes the same stance. Through competition law, large (internet) companies such as Facebook, Microsoft, and google can be tackled for abusing their dominant position. It is not without reason that the European Data protection Supervisor, among others, has stressed that that in Big Data processes there will often be a confluence of data protection, consumer protection, and competition law.

For that reason, there have been calls for increased cooperation between the administrative authorities responsible for the supervision of compliance within these fields of law. In the Netherlands, the relevant authorities are the Autoriteit Persoonsgevens (the Data Protection Authority) and the Autoriteit Consument en Markt (the Authority for Consumers & Markets).

The question becomes to what extent is it realistic for these three legal fields to play a major role in horizontal relationships; it is apparent that diagonal relationships (the relationship between citizens and large commercial entities) can be placed within this framework, but this is not the case with the relationship between citizens. Even if supervisory authorities would be able to enforce these requirements in all horizontal relations, it is both impractical and likely undesirable for governmental agencies or public officials to monitor the everyday use of everyday products in horizontal relationships such as smartphones, drones and IoT devices.

Civil law
Civil law in both the Netherlands and the countries analyzed for this research provides many opportunities for enforcement action against violations of horizontal privacy. The most important enforcement action can be found in tort law. If the victim of a horizontal privacy violation suffers harm, the defendant has an obligation of compensation. This does not only apply to pecuniary damages, but on the basis of article 6:106 of the Dutch Civil Code and the associated jurisprudence, it also applies to harm to reputation and immaterial damages. However, the mere violation of the right to privacy will not immediately result in a right to compensation; it must either be a gross violation from which it is to be expected that damage will follow, or the plaintiff must be able to substantiate that harm was caused.

Civil law has two limitations with regard to the protection of horizontal privacy. First, civil law is primarily reactive in nature and while it is possible to proactively take action against horizontal privacy violations, such as the prohibition of unlawful press publications, it will often not be known in advance that a citizen will commit a privacy violation. In that event, the enforcement action remains with tort law to retroactively obtain compensation for any harm caused. The second limitation lies in the possibilities for the injured party to actually exercise his or her rights. Proceedings before a court are costly and the outcomes are unclear. Horizontal privacy violations are in many cases committed anonymously or through the use of pseudonyms on the Internet, making independent actions by citizens even more difficult. The problem of difficult or costly litigation is partially addressed by the possibility of collective proceedings, although this option is only available for a limited category of privacy infringements.

Finally, it should be noted that going to civil court (or filing a criminal complaint) is not always a realistic option for injured parties. In sensitive cases, such as the distribution of nude images, the victim may choose not to go to court because of the inevitable confrontation with the culprit and the openness of the court proceedings. In a twist of irony, the procedure could cause a continuation or further aggravate the violation of privacy. Shielded or non-public procedures could address these problems, although at the cost of the openness and transparency of the judicial system.

The role of producers, distributors, and internet intermediaries

Liability of producers and distributors
In the Netherlands and most countries analyzed during this study, we have not come across any legal provisions prohibiting certain types of products (such as eavesdropping devices, spycams, stalkerware) in advance or the setting out of specific rules for their sale. It is only Germany who has a (limited) ban on the use of equipment that can (also) be used to eavesdrop on individuals. In addition, under the rules on product liability, no action can be taken against producers of hardware and software, even if they are clearly intended to commit violations of horizontal privacy.

Liability of internet intermediaries
With regards to the role of internet platforms in combating horizontal privacy violations, the question is to which extent they are liable for the behavior of their users and what their corresponding responsibility is to prevent the commission of these violations. According to the current European regulations (specifically, the e-Commerce Directive), the fundamental principle is that internet platforms are not liable if they are not aware (or should have been aware) that unlawful conduct has taken place and they act promptly to remove the infringing material in question once they do become aware.

For the time being, it appears that parties such as Facebook and Twitter can invoke their exemptions of liability under Article 14 of the e-Commerce Directive with respect to content posted by users. Pursuant to Article 15 of the same Directive, these internet platforms are also not obligated to proactively monitor their platforms for harmful content. However, they may be required by national courts to implement measures to prevent future violations, despite the harm having already been caused. It is questionable whether this sufficiently solves the problem of horizontal privacy violations, because the measures must concern the removal of content that is identical or similar to that which has already been brought before the courts. This means that a court ruling will be necessary for each violation of horizontal privacy.

In order to stimulate internet platforms to increase their enforcement actions, there might be room to consider the introduction of a good Samaritan clause (as proposed in the Communication on combating illegal content online). A potentially harmful side effect of such a clause would be to provide internet platforms with more power and control over the content placed on their platforms. They will enjoy more 'editorial freedom' without any of the corresponding liability. If the route of introducing a good Samaritan clause is pursued, it will be important to delineate the corresponding responsibilities and limits of such a clause.

A more far-reaching step is the introduction of a proactive duty of care. The ECtHR in its *Delfi* ruling did not preclude the taking of proactive measures, although this case was in the context of another type of internet service (a message forum which belonged to a major internet portal providing daily news). The Member States of the European Union are currently working on changing the liability regime for internet intermediaries through the Digital Services Act. It is expected to include a 'duty of care' for internet platforms, although its precise meaning and what it will entail are not yet clear.

The introduction of a possible duty of care to help address violations of horizontal privacy highlights another challenge. In contrast to works protected by copyright, it is often difficult to determine when a privacy violation has taken place. Expressions and their effect on the privacy of a data subject are strongly context specific. This complicates the ability of intermediaries to assess whether an expression is unlawful, especially when they are made on a large scale and therefore its detection is likely to be automated. This may result in internet platforms preferring to choose broad parameters to avoid liability, which will consequently have a negative impact on the freedom of expression.

Germany appears to take a much stricter approach to dealing with illegal online content; through the *Netzwerkdurchsetzungsgesetz* (the Network Enforcement Act). Sweden, through its interpretation of the old BBS legislation, also has legal possibilities to hold internet platforms liable for criminal violations of horizontal privacy. It can be said that the legal 'stick' through which rapid and effective action can be taken against violations committed on internet platforms is more readily present in Sweden and Germany, as opposed to the Netherlands. However, it remains dependent on whether it concerns a violation of horizontal privacy that is criminalized.

In addition to measures taken by internet platforms themselves (such as the removal, blocking, or filtering of content), users can also take action against violations of their privacy. Individuals can, on one hand, exercise their rights under the GDPR (in particular, the right to erasure as set out in Article 17 of the GDPR) and, on the other hand, leverage the possibilities offered by the Civil Code (e.g. through an action in tort law).

The problem with exercising these rights is that the injured party must focus primarily on the internet platforms instead of the user who committed the violating act. Particularly when it comes to obtaining compensation, this raises the threshold that injured parties need to meet in order bring an action because they will first be required to go through proceedings against the platform (e.g. to obtain user data) before they can start proceedings against the user who committed the violating act.

Other mechanisms

In addition to laws and regulations, there are other available mechanisms aimed at regulating privacy in horizontal relationships. These mechanisms concern self-regulation, awareness and education.

Self-regulation

While we (as researchers) have less insight into initiatives in smaller social contexts, self-regulation seems to be particularly focused around online services. Self-regulatory initiatives by producers and distributors of hardware and software that is specifically suited to infringe privacy have not been found.

Self-regulatory initiatives to protect privacy in horizontal relationships are of particular relevance in the context of online services. These are internet platforms and other service providers that work independently or in a public-private context to regulate online content. Public-private initiatives to regulate online content are focused on child abuse images, racist or xenophobic content (hate speech), and terrorist content (glorification or incitement of terrorism). Other violations of horizontal privacy (such as the communication

of insults or revenge pornography) are mainly regulated by internet service providers through community standards and abuse policies.

Although self-regulation through Terms of Use can be a powerful tool to counter horizontal privacy violations, there are also concerns about potential and undesirable side-effects. For example, the UN Special Rapporteur on Freedom of Expression warned that internet platforms can regulate themselves too independently on the basis of their community standards.

Awareness and Education
In the field awareness and education, there is a fairly uniform picture when looking at the different European countries analyzed for this study. This can be partly attributed to the fact that a lot of awareness raising iniatives, especially information directed at children, is coordinated at a European level. This enables countries to adopt successful campaigns from each other and exchange lessons learned.

Overview of standardization and legal protection of horizontal privacy
On the basis of our research, we set out the following overview of violations and the associated standards and legal protection:

Standardization and the legal protection of privacy in horizontal relationships						
Type of violation	**Examples**	**Standards and protection**				
		Laws and regulations				Other mechanisms(self-regulation)
		Criminal law	Data protection law	Administrative law, Competition law, and Consumer protection law	Civil law	
Observation, collection, and registration	Voyeurism, (covert) video surveillance, eavesdropping,use of spyware and stalkerware, fencing information, filming of victims	Computer hacking (138ab Sr), overname gegevens (138c Sr), eavesdropping (139c Sr), covertly recording conversations (139a, b Sr), covert camera surveillance (139f Sr), data fencing (139e, g Sr), harassment (285 Sr)	Illegitimate processing, right to erasure (Article 17 GDPR)	Administrative law (APV), consumer protection, product safety, unfair trade practices	Tortious act, violation of portrait rights	*Naming and shaming*

Analysis and decision-making	Profiling and automated decision-making		Illegitimate processing, right to erasure (Article 17 GDPR), ban on automated decision-making (Article 22 GDPR)	Consumer protection	Tortious act	
Creation and sharing	Insults, *deepfakes*, false advertising. attribution of expression to an individual, identity theft, revenge pornography	Defamation, incitment and hate speech (137c en d Sr), insult (266 Sr), libel (261 Sr), slander (262 Sr), revenge porn (139h Sr),	Illegitimate processing, right to rectification (Article 16 GDPR), right to erasure (Article 17 GDPR)	-	Tortious act, rectification right, portrait rights.	Violating Terms of Use of platforms, *naming and shaming*
Interaction and communication	Stalking, threats, *sextortion*, cyber-bullying. (further: insults, libel, slander)	285 Sr, threats (317 Sr), revenge porn (139h Sr), fraud (225 Sr, 326 Sr)	Illegitimate processing, right to rectification (Article 16 GDPR), right to erasure (Article 17 GDPR)	-	Tortious act,	Violating Terms of Use of platforms, *naming and shaming*

Integrating foreign legal concepts into the legal order of the Netherlands

Our research has shown that the regulation of horizontal privacy in the legal system of the countries analyzed is more or less the same. The ability to adopt 'lessons learned' in this case is limited. Legal concepts that might contribute to better protection of horizontal privacy lie primarily in criminal law and the rules addressing the liability of internet platforms.

A first criminal provision that can be considered is the broader criminalization for the publication and distribution of offensive or obscene content, following the example of Poland and the United Kingdom. The main advantage of this possibility is the increased degree of flexibility for government to act autonomously in the enforcement of standards. Although, it brings with it a major risk in that its introduction will create legal uncertainty. In the absence of a clear definition and delineation of material considered to be obscene, offensive, hurtful or otherwise harmful, there will always be a risk of censorship or arbitrary enforcement.

A second criminal provision that may qualify for integration into Dutch criminal law is the filming of individuals in need of assistance. Introducing a ban on the filming of individuals requiring assistance will have a potential effect on the freedom of expression. If the provision is sufficiently qualified and provides exemptions in the context of, for example, the press, it is likely that an appropriate balance can be struck between the right to privacy and the right to freedom of expression. Another consequence that should be taken into account is that images of bystanders can contribute to clarifying the alleged crime or to better understand the circumstances surrounding an accident. In the context of potentially broadening criminalization, these are important considerations to take into account.

If the legislator chooses to impose stricter requirements on internet platforms, the German Network Enforcement Act can serve as an example. Although the consequences of the law (both positive and negative) have not yet been clearly established, it can be expected that such provisions affect the freedom of expression. Additionally, measures aimed at internet platforms can also affect the freedom of enterprise and potentially influence the economic climate and innovation in the Netherlands.

Legal concepts not borrowed from abroad

While certain legal concepts can be borrowed from abroad, there are number of proposals that have emerged from our own analysis of Dutch and foreign legal protection.

A first option is the exploration of stricter requirements for the sale of products and services that are primarily made to infringe the private life of individuals. Prime examples include spycams, monitoring beacons, and stalkerware. Restrictions could be placed on the sale of such products to private individuals, additional notification requirements could be introduced, or a licensing system for sellers and/or users. These measures stop short of a complete ban.

Second, the extent to which technical requirements could be imposed to make certain recordings impossible (or, in any case, substantially more difficult) could also be a topic worthy of exploration. This could for instance include geo-fencing with regard to 'no-fly zones' for drones, or the automatic blurring of faces when using cameras in specific areas. There could also be a further investigation into the extent to which technical requirements can be imposed on products in order to reduce their stealthy nature. An example is the mandatory issuing of a sound or light signal when a products start recording. By referring to Article 25 of the GDPR, there is already a (potential) legal basis for the enforcement of such measures.

Future regulation of horizontal privacy violations

When it comes to legal measures aimed at providing better protection for horizontal privacy, there are roughly two options to choose from: (1) take measures aimed reducing the opportunities to violate privacy (*ex ante*, preventative measures), and (2) take measures aimed at more effectively ending privacy violations and compensating victims (*ex post*, reactive measures).

The first option and category of measures may include banning certain products or services or making the sale or purchase of such products subject to licensing requirements as described above. A drawback of this approach is that most products (e.g. smartphones or drones) can be used for both legitimate and illegal purposes. This makes it problematic to prohibit certain products or services in advance or to further regulate their sale and use.

The option of *ex post* regulation brings with it the advantage that the lawful application and use of technology are not prohibited beforehand. However, the associated disadvantage is that the applications are so diverse that it is virtually impossible to test the legitimacy all potential uses of technology in horizontal relationships (either by citizens themselves, or by civil rights organizations or governmental bodies). Furthermore, the harm has already been caused by the time legal action can be taken. At best, the citizen can recover damages, although it will often prove difficult, because: (i) the culprit cannot always be

identified due to obstacles in obtaining evidence, (ii) the harm and corresponding damages are not quantifiable or easy to interpret, and/or (iii) the individual simply does not wish to draw even more attention to what has been exposed with the invasion of his or her privacy.

A compromise would be to not focus on the commission of the privacy violation but rather on the further dissemination of unlawfully obtained information about other citizens. internet services and platforms in particular have an important role to play in this respect. The question becomes to what extent these platforms (should) play a proactive role to prevent violations of horizontal privacy. While a general duty of care already exists, it remains in many regards unclear how far it applies in the digital context.

Legal protection in practice

Although the horizontal application of fundamental rights is recognized, the notion that the parties involved are more or less equivalent and therefore should be able to sort any issues amongst themselves remains. Although testing the effectiveness of privacy protection measures was not the assignment for this study, the result is that we can question the level of actual legal protection provided to citizens. On one hand, it is difficult for citizens to take action against violations of their right to privacy, while on the other hand, the capacity of the government (such as the police, judiciary, and regulators) to enforce the current standards is limited. Possible reinforcement of the right to privacy in legislation and further regulations can therefore never be considered in isolation from the actual challenges faced by citizens or the capacity of the government in its enforcement.

It is also important to focus on the development of societal norms in the digital context. In contrast to the physical world, the norms in the digital world have not yet been fully developed. The relative absence of authoritative institutions also play a role in the emergence and persistence of privacy violations. Awareness and self-regulation can help to form and maintain norms and values in places where governmental presence is less pronounced.

More generally, it can be stated that it is precisely in the digital environment that the legislator must invest in mechanisms to, at an early stage, identify technological developments, new applications, and their consequences. If legislation is delayed for years, by the time a new law or provision enters into force, the technology that was supposed to be addressed is already out of fashion or has become so widespread and widely used that it becomes impossible to set any substantial or meaningful limits to it. In view of the great importance of digitization of the Netherlands, continued discussion on technological developments and their impact on society, for instance through a Parliamentary Committee on the Digital Future, is advised.