CONSIDERATI

Info@considerati.com
www.considerati.com
020 73 70 069
De Boelelaan 7, Amsterdam

Het recht op privacy in horizontale verhoudingen

WODC

Datum: 12 juli 2020

Bart W. Schermer
Considerati

Bart van der Sloot
Tilburg University

Colofon

Inhoudsopgave

Gebruikte afkortingen

ACM	Autoriteit Consument en Markt
APV	Algemene Plaatselijke Verordening
AVG	Algemene Verordening gegevensbescherming
BBS	Bulletin Board System
BDSM	Bondage and Discipline, Dominance and Submission
BOA	Buitengewoon Opsporingsambtenaar
BVerfGE	Bundesverfassungsgericht
EHRM	Europees Hof voor de Rechten van de Mens
EHvJ	Europees Hof van Justitie
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
GPS	Global Positioning System
GSM	Global System for Mobile communications
HRA	Human Rights Act
IM	Instant messaging
IoT	Internet of Things
ISP	Internet Service Provider
IVBPR	Internationaal Verdrag Inzake de Burgerlijke en Politieke Rechten
LHBT	Lesbisch, homoseksueel, biseksueel, transgender
NGO	Non gouvernementele organisatie
NMA	Nederlandse Mededingingsautoriteit
SMS	Short Message Service
SNS	Social Network Site
UVRM	Universele Verklaring van de Rechten van de Mens

1 Inleiding

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.[1] 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 (verder: de initiatiefnota) wordt het probleem van privacyschendingen in horizontale verhoudingen gesignaleerd.[2] 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.[3] In de initiatiefnota worden tal van oplossingsrichtingen geopperd om de privacybescherming in horizontale verhoudingen te versterken. In 2018 heeft de Kamer de regering gevraagd om nader werk te maken van het verkennen van deze deeloplossingen.[4] In juni 2019 heeft de Minister voor Rechtsbescherming zijn visie op de bescherming van privacy in horizontale verhoudingen uiteengezet.[5] Een van de actiepunten betreft een onderzoek naar horizontale privacy en 'informationele zelfbeschikking'. Meer specifiek moest door middel van rechtsvergelijkend onderzoek worden gekeken in hoeverre er aangrijpingspunten zijn voor de aanvulling en verdere verbetering van de horizontale privacybescherming in Nederland. Dit rapport vormt de uitwerking van deze rechtsvergelijking.

1.1 Probleemstelling

In dit onderzoek staat de vraag centraal wat 'horizontale privacy' is en hoe het in Nederland (beter) beschermd kan worden.

Voor dit onderzoek geldt een drieledige probleemstelling:

- 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?

[1] Ter illustratie van de ernst en omvang van dit probleem: in 2019 hebben 2400 jongeren zich met een hulpvraag betreffende (afpersing met) online naaktbeelden gewend tot het expertisebureau online kindermisbruik (zie: https://www.eokm.nl/wp-content/uploads/2020/05/jaarverslag-2019.pdf)
[2] Kamerstukken II, 2017/2018, 34926 nrs. 1-2 (Initiatiefnota onderlinge privacy)
[3] Kamerbrief Horizontale Privacy, p. 1
[4] Kamerstukken II, 2017/2018, 34926, nr. 4
[5] Kamerstukken II, 2018/2019, 34926, nr. 8

1.2 Vraagstelling

Om de voor het oplossen van de probleemstelling noodzakelijke rechtsvergelijking mogelijk te maken worden de volgende deelvragen in dit rapport beantwoord:

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

1.3 Aanpak

Voor dit onderzoek hanteren wij de volgende aanpak:

1.3.1 Conceptuele analyse

Om tot een goede rechtsvergelijking te komen is het zaak om het begrip horizontale privacy nader te duiden. Door middel van een conceptuele analyse krijgen we inzicht in het begrip horizontale privacy en de potentiële bedreigingen van de privacy in horizontale verhoudingen. Vervolgens kijken wij hoe horizontale privacy momenteel genormeerd en gereguleerd is in Nederland. Hierbij kijken wij naar wetgeving die privacy in horizontale verhoudingen borgt (gegevensbeschermingsrecht, strafrecht, civiel recht *et cetera*) en naar zelfregulering door maatschappelijke actoren.

De conceptuele analyse geeft een begrenzing van het begrip horizontale privacy en een categorisering van de verschillende elementen die bij het vraagstuk van horizontale privacy een rol spelen (te beschermen belangen, bedreigingen en regulering). De categorisering ziet op (tenminste) de volgende elementen:

1. De aard van de inbreuk op de privacy van burgers in horizontale verhoudingen;
2. Concrete verschijningsvormen van deze inbreuken (voorbeelden);
3. De wijze waarop deze inbreuken zijn genormeerd binnen verschillende wetten en regels;
4. De wijze waarop via deze wetten en regels handhaving wordt afgedwongen.

1.3.2 Rechtsvergelijking

Het verzamelen van de gegevens ten behoeve van de rechtsvergelijking is primair uitgevoerd door landenrapporteurs.[6] Op basis van de uit de conceptuele analyse verkregen categorisering is de landenrapporteurs gevraagd om een rapportage op te leveren welke de basis vormde voor het rechtsvergelijkend onderzoek. Deze rapportages zijn bijgevoegd in de bijlagen bij dit rapport. De landenrapportages zijn aangevuld met eigen deskresearch waar nuttig of noodzakelijk.

Voor de rechtsvergelijking zijn Duitsland, Polen, het Verenigd Koninkrijk en Zweden gekozen. Relevante factoren bij de selectie van de landen voor de rechtsvergelijking waren verschillen in culturele tradities, verschillen in rechtssystemen en geografische spreiding. In onze rechtsvergelijking was Spanje aanvankelijk betrokken als Zuid-Europees land. In verband met de Covid19 crisis is de Spaanse rapporteur er echter niet in geslaagd binnen de termijn een rapportage op te leveren, waardoor wij niet in staat zijn geweest Spanje volwaardig in de rechtsvergelijking te betrekken. Als alternatief is een 'quick scan' voor Italië gedaan. Waar relevant worden de resultaten daarvan in het onderzoek weergegeven.

Duitsland

Duitsland wordt specifiek als voorbeeld genoemd in de initiatiefnota en de startnotitie voor dit onderzoek. Aldus ligt het in de rede Duitsland te betrekken in de rechtsvergelijking. Met name het concept van de *Informationelle Selbstbestimmung*, als specifieke uitwerking van het Duitse grondwettelijk vastgelegde persoonlijkheidsrecht (artikel 2 lid 1 jo. artikel 1 lid 1 *Grundgesetz*), is relevant voor het onderzoek. Door de grondrechtelijke bescherming van het recht op 'informationele zelfbeschikking' en de mogelijkheid tot grondwettelijke toetsing door de rechter is binnen de Duitse rechtspraktijk mogelijk een meer fundamentele stellingname op het gebied van horizontale privacy ten opzichte van Nederland, welke interessant is om te onderzoeken.

Polen

Polen is gekozen als Oost-Europees land, met name omdat Polen een relatief jonge grondwet heeft waarin de horizontale werking van grondrechten expliciet wordt erkend. Als zodanig is het interessant om te zien wat dit betekent voor de rechtsbescherming *in concreto*. Verder kent het Poolse recht een brede strafbaarstelling van heimelijk filmen, fotograferen en afluisteren.[7]

Zweden

Zweden is gekozen vanuit de Scandinavische landen omdat het een *civil law* traditie heeft die sterk beïnvloed wordt door jurisprudentie.[8] In het constitutionele recht ligt verder een sterke nadruk op de vrijheid van meningsuiting, wat mogelijk tot andere afwegingen leidt met betrekking tot het belang van de bescherming van privacy in horizontale verhoudingen.

[6] De landenrapporteurs zijn geworven uit de academische netwerken van de onderzoekers. Hierbij is rekening gehouden met de specifiek benodigde expertise op het gebied van privacy en gegevensbescherming. Bij de selectie van de rapporteurs en de landen speelde ook de praktische overweging mee welke landenrapporteurs bereid en beschikbaar waren.
[7] Zie: Koops, B.J. *et al.* (2018), The reasonableness of remaining unobserved. A comparative analysis of visual surveillance and voyeurism in criminal law, in: *Law & Social Inquiry*, 18 January 2018, DOI: 10.1111/lsi.12348
[8] Bogdan, M. (2000), *Swedish Law in the New Millennium*, Nordstets Juridik

Het Verenigd Koninkrijk[9]

Het Verenigd Koninkrijk is interessant omdat het een common law traditie heeft, in plaats van een continentale traditie (civil law). Hierdoor zijn er mogelijke interessante verschillen met de continentale rechtstraditie als het gaat over de regulering van horizontale privacy. Verder kent het Verenigd Koninkrijk een actieve en competente privacy toezichthouder, de Information Commissioner's Office, die meer dan andere Europese toezichthouders actief adviseert over de naleving en interpretatie van de Algemene verordening gegevensbescherming (AVG) en de UK Data Protection Act 2018. Tenslotte heeft het Verenigd Koninkrijk pas relatief recent mensenrechten vastgelegd in de nationale rechtsorde met de Human Rights Act 1998.

1.3.3 Analyse en synthese

In de fase van analyse en synthese bekijken wij hoe de juridische normering van horizontale privacy in de onderzochte landen overeenkomt met de normering in Nederland en waar deze afwijkt. Op basis van deze vergelijking kunnen we bepalen in hoeverre de rechtsbescherming in Nederland nog verder verbeterd kan of moet worden. Hierbij kunnen interessante in het buitenland gevonden rechtsfiguren dienen ter inspiratie.

1.3.3.1 Expertbijeenkomst

In de analyse en synthese fase zijn de bevindingen van de onderzoekers voorgelegd aan een aantal experts in een online expertmeeting. Een overzicht van de deelnemers is bijgevoegd in de bijlagen.

1.4 Scope

Aantastingen van de persoonlijke levenssfeer in horizontale verhoudingen vinden op talloze manieren plaats. Denk aan fysieke schendingen zoals het binnendringen van iemands woning of aan digitale schendingen zoals het online plaatsen van privéfilmpjes. Binnen de context van dit rapport richten wij ons specifiek op de digitale schendingen van de privacy. In dit onderzoek besteden wij aandacht aan de relatie burger-burger en aan de relatie burger-private rechtspersoon (meer specifiek burger-bedrijfsleven). Wel ligt de nadruk in het onderzoek op het bespreken en analyseren van privacyschendingen tussen burgers onderling. Dit met het oog op de vraagstelling van dit onderzoek die mede voortvloeit uit de Initiatiefnota Koopmans.[10]

1.5 Leeswijzer en hoofdstukindeling

In hoofdstuk 2 schetsen wij het probleem van privacyschendingen in horizontale verhoudingen. In dit hoofdstuk categoriseren wij horizontale privacyschendingen op basis van handelingen die de persoonlijke levenssfeer kunnen aantasten en hun concrete verschijningsvormen (wraakporno, heimelijk cameratoezicht, belediging *et cetera*).

In hoofdstuk 3 analyseren wij de belangen en waarden die in het geding kunnen komen bij horizontale privacyschendingen.

[9] Feitelijk gaat het om een analyse van het recht van Engeland, Schotland, Wales en Noord-Ierland. In deze rapportage ligt de nadruk op Engeland tenzij anders aangegeven. Voor een volledig overzicht zie de bij dit rapport behorende landenrapportage.
[10] Kamerstukken II, 2017/2018, 34926 nrs. 1-2 (Initiatiefnota onderlinge privacy)

In hoofdstuk 4 verkennen wij hoe de grondwettelijke bescherming van het recht op privacy zich in Nederland en Europa heeft ontwikkeld.

In hoofdstuk 5 ligt de focus op de vraag in hoeverre grondrechten horizontale werking hebben. In dit hoofdstuk kijken wij ook hoe deze horizontale werking gestalte krijgt binnen de Nederlandse rechtsorde en de landen die geselecteerd zijn voor de rechtsvergelijking.

In de hoofdstukken 5 tot en met 9 verkennen wij hoe privacybescherming in horizontale verhoudingen concreet gestalte krijgt in verschillende rechtsgebieden zoals gegevensbeschermingsrecht, het strafrecht, het administratief recht en het civiel recht.

In hoofdstuk 10 gaan wij in op de rol en positie van producenten, distributeurs en internettussenpersonen bij horizontale privacyschendingen. We analyseren hoe zij gedragingen tussen burgers onderling normeren en reguleren, bijvoorbeeld door middel van hun gebruiksvoorwaarden. Ook bespreken we hun mogelijke aansprakelijkheid voor horizontale privacyschendingen.

In hoofdstuk 11 bespreken wij andere mechanismen dan wetgeving om privacy in horizontale verhoudingen te normeren en te beschermen. Het gaat dan primair om zelfregulering, onderwijs en voorlichting.

In hoofdstuk 12 bieden wij een schematisch overzicht van de normering en beschermingsmechanismen zoals deze in de voorgaande hoofdstukken zijn besproken.

In hoofdstuk 13 analyseren we de belangrijkste knelpunten bij de bescherming van de horizontale privacy en bespreken we de belangrijkste verschillen en overeenkomsten tussen de verschillende rechtssystemen. Op basis daarvan kijken we of er interessante rechtsfiguren in het buitenland zijn die ‘getransplanteerd’ kunnen worden in Nederlandse context. Ook bespreken we de eventuele negatieve effecten daarvan.

Hoofdstuk 14 bevat de samenvatting en belangrijkste conclusies van ons onderzoek.

2 Privacyschendingen in horizontale verhoudingen: een probleemschets

2.1 Achtergrond

Het begrip 'horizontale privacy' (ook wel 'onderlinge privacy'), verwijst naar het recht op bescherming van de persoonlijke levenssfeer in min of meer gelijkwaardige relaties. Hierbij moet primair worden gedacht aan burgers onderling (natuurlijke personen), maar ook aan de verhouding tussen burgers en bedrijven, stichtingen of verenigingen (private rechtspersonen).

Digitalisering in het algemeen en de opkomst van het internet in het bijzonder hebben ontegenzeggelijk geleid tot een toename van privacyschendingen in horizontale verhoudingen (verder ook: horizontale privacyschendingen). Burgers hebben toegang tot tal van middelen die gebruikt kunnen worden om bewust of onbewust de privacy van medeburgers te schenden. Denk aan mobiele telefoons, *drones*, *spycams*, slimme apparaten (*Internet of Things*) en sociale media. Met deze middelen worden burgers geobserveerd, (persoons)gegevens vastgelegd en beelden gedeeld. Hierdoor krijgen derden toegang tot gegevens waar zij geen toegang toe zouden moeten hebben en/of worden gegevens buiten hun originele context gebruikt.[11]

Er zijn vele horizontale privacyschendingen (wraakporno, heimelijk observeren, online belediging) te bedenken. Om tot een zekere ordening te komen, onderscheiden wij de handelingen die leiden tot een privacyschending (observeren, vastleggen, delen *et cetera*) en de mogelijke consequenties van deze handelingen. Bij dat laatste gaat het met name om de belangen en waarden die geraakt worden door de privacyschending (op individueel en maatschappelijk niveau).

2.2 Handelingen die de persoonlijke levenssfeer kunnen raken

De persoonlijke levenssfeer van burgers kan op diverse manieren worden geschonden. Zo zal het delen van privégegevens een schending van de privacy opleveren, maar ook het enkele observeren (of zelfs het idee dat je geobserveerd wordt) kan een privacyschending zijn. In deze paragraaf beschrijven wij handelingen die kunnen leiden tot een schending van de horizontale privacy.

2.2.1 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.

Een specifiek aspect dat in het kader van het observeren van personen steeds relevanter wordt is de automatische herkenning van personen op basis van biometrische gegevens. Denk hierbij aan

[11] Voor een bespreking van het probleem van 'contextvervaging' en 'contextverval' zie onder andere: Boyd, D. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In: Z. Papacharissi (Ed.), *A networked self: Identity, community, and culture on social network sites* (pp. 39–58). New York: Routledge

vingerafdrukken of gezichtsherkenning. Hoewel biometrie vooralsnog voornamelijk wordt toegepast door overheden en bedrijven in het kader van beveiliging, zien we ook de toepassing van biometrie door burgers. Denk hierbij bijvoorbeeld aan gezichtsherkenning die gebruikt wordt om mensen automatisch te herkennen en te *taggen* in foto's op sociale media.[12]

Een specifieke vorm van observatie is het gebruik van *stalkerware*. Dit zijn apps die geïnstalleerd worden op de telefoon van een persoon en de gebruiker in staat stellen om het gebruik van de telefoon te monitoren. Het gaat dan om de observatie (en eventueel vastlegging) van een veelheid aan privacygevoelige informatie zoals de gesprekken die een persoon heeft gevoerd (spraak en tekst), de locatie van een persoon (GPS), de foto's die met de telefoon zijn genomen en contactgegevens.

2.2.2 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.

2.2.3 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. Het doel daarvan is doorgaans het analyseren van gedrag teneinde beter geïnformeerde beslissingen te kunnen nemen. Hierbij kan het ook gaan om (geautomatiseerde) besluiten over personen. Denk bijvoorbeeld aan het beoordelen van de kredietwaardigheid van een persoon, het gericht tonen van advertenties, of het inschatten van de waarde van een klant.

2.2.4 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.

Een relatief nieuwe vorm van creatie die tot een horizontale privacyschending kan leiden is de *deepfake*.[13] Bij een *deepfake* worden met behulp van kunstmatige intelligentie (bewegende) beelden gecreëerd van een bestaand persoon die nagenoeg niet van echt zijn te onderscheiden. Deze technologie kan bijvoorbeeld gebruikt worden om een persoon iets te laten zeggen dat hij of zij in het echt nooit gezegd heeft.

2.2.5 Delen

Bij veel horizontale privacyschendingen is er sprake van het delen van gegevens (foto's, tekst, video's of geluid). Gegevens kunnen worden gedeeld met één persoon, een (relatief) beperkte groep (zoals

[12] Voor een beschrijving van de privacyrechtelijke aspecten van gezichtsherkenning zie: Keymolen, E., *et al.* (2020), *Op het eerste gezicht: Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties*, WODC projectnummer 2992
[13] Zie bijvoorbeeld: Maras, M. H., Alexandrou, A. (2019), Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos, in: *International Journal of Evidence and Proof*, Volume: 23 issue: 3, p. 255-262

bijvoorbeeld met een afgesloten WhatsApp groep), of met een grote en in beginsel ongedefinieerde groep (zoals bijvoorbeeld via Facebook, Instagram of Twitter). Door het delen van gegevens wordt informatie over een persoon, of de identiteit van een persoon (ongewenst) openbaar. Hoewel gegevens bewust gedeeld kunnen worden om iemand schade toe te brengen (zoals in het geval van wraakporno), hoeft er bij delen zeker geen boos opzet in het spel te zijn. Zo delen mensen gegevens van anderen zonder daar de mogelijke negatieve gevolgen van in te zien, of delen zij beelden van zichzelf waarin ook anderen zichtbaar zijn (denk bijvoorbeeld aan het delen van een foto waar meerdere personen op staan). Een relatief nieuw fenomeen is ouders die bovenmatig gegevens van hun kinderen delen via sociale media (*sharenting*).[14]

Ook bedrijven delen gegevens met elkaar (denk bijvoorbeeld aan het verkopen van een klantenbestand). Doorgaans betekent dit niet de openbaarmaking van deze gegevens. Wel kan gesteld worden dat de betrokkene hierdoor de controle over zijn of haar persoonsgegevens verliest.[15]

2.2.6 Interactie en communicatie

Directe interactie en communicatie met een persoon kan ook diens privacy 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. Extreme vormen van negatieve interactie zoals bedreiging, digitale *stalking* en cyberpesten leveren een schending van de horizontale privacy op, maar ook 'lichtere' varianten, zoals belediging en *trolling*[16] kunnen een horizontale privacyschending opleveren.

2.3 Technologische en maatschappelijke ontwikkelingen[17]

Horizontale privacyschendingen zijn geen nieuw fenomeen. Wel kan gesteld worden dat door een aantal technologische en maatschappelijke ontwikkelingen horizontale privacyschendingen een groter probleem zijn geworden. In deze paragraaf bespreken wij een aantal trends en hun invloed op het vraagstuk van de horizontale privacy.

2.3.1 Democratisering opnametechnieken

Allereerst maken moderne digitale middelen het mogelijk om grote hoeveelheden informatie te verzamelen. Sensoren (camera's, microfoons, warmtemeters) worden steeds vaker ingebouwd in alledaagse objecten, zoals horloges, deurbellen, koelkasten en telefoons. Platformen voor deze sensoren zoals *drones* en *smartphones* zijn steeds beter beschikbaar en worden steeds goedkoper. Daarbij komt dat sensoren kleiner worden en makkelijk te verbergen. Zodoende kunnen er heimelijk opnames worden gemaakt. Sensoren worden niet alleen ingezet door grote bedrijven en overheidsinstanties, ook burgers

[14] Zie bijvoorbeeld: Steinberg, S. B. (2017), Sharenting: Children's privacy in the age of social media, in: *Emory Law Journal*, vol 66-839, p. 839-884
[15] Zie in dit kader: ECLI:NL:RBOVE:2019:1827 en ECLI:NL:RVS:2020:899
[16] De Urban dictionary omschrijft trolling als: *"the deliberate act (…) of making random unsolicited and/or controversial comments on various internet forums with the intent to provoke an emotional knee jerk reaction from unsuspecting readers to engage in a fight or argument"*. Via: https//www.urbandictionary.com.
[17] Deze paragraaf leent uit en bouwt deels voort op de bevindingen uit het WODC rapport 'Waarborgen tegen privacyrisico's hobbydrones & spionageproducten', WODC projectnummer 3063

maken er steeds meer gebruik van. Dat heeft met name twee oorzaken. Ten eerste zijn de producten steeds beter en algemener beschikbaar. Waar dergelijke producten vroeger hoofdzakelijk in gespecialiseerde winkels te koop waren, is gespecialiseerde apparatuur momenteel eenvoudig te bemachtigen via Bol.com, Amazon.nl en een myriade aan Chinese webshops. Ten tweede dalen de kosten steeds verder, zodat economische belemmeringen voor de aanschaf en het gebruik van deze producten vrijwel volledig zijn verdwenen. Beide ontwikkelingen hebben een democratisering van 'spionageproducten' tot gevolg gehad.

2.3.2 Verbeterde opnametechnieken

Naast een sterke kwantitatieve stijging van het gebruik van apparatuur met sensoren door burgers, zijn ook de nodige kwalitatieve veranderingen zichtbaar. Ten eerste worden de steeds kleinere sensoren in allerlei alledaagse objecten, zoals shampooflessen of knuffels, ingebouwd. Dit maakt het eenvoudiger om anderen binnen intieme ruimtes en sferen te observeren. Ten tweede worden de opnametechnieken steeds preciezer, waardoor niet alleen de kwaliteit en resolutie van het opgenomen beeld en geluid beter wordt; ook de afstand waarop personen bespied kunnen worden neemt toe. Ten derde kunnen spionageproducten zich steeds beters langs fysieke barrières wurmen: zo kunnen sommige sensoren geluid of infrarood door de muren van een huis heen opnemen.

2.3.3 Hardware en software

Winkels verkopen allerhande spionage apparatuur, zoals objecten met een GSM zender, GPS *trackers* die op objecten of personen kunnen worden vastgemaakt (peilbakens), rookmelders met camera's, pennen met de mogelijkheid om geluidsopnames te maken, camera's in camouflagekleuren en opritverklikkers met bewegingsdetectie. Naast dergelijke hardware wordt ook software verkocht die burgers in staat stelt hun medeburgers in de gaten te houden (*stalkerware*). Zo wordt controlesoftware aangeprezen als instrument om kinderen en werknemers in de gaten te houden. Dergelijke software biedt talloze mogelijkheden zoals het kopiëren van alle inkomende en uitgaande berichten (email, WhatsApp, SMS), het doorsturen van de surfgeschiedenis, het volgen van een persoon aan de hand van de in de telefoon ingebouwde GPS, het opnemen van alle gesprekken die gevoerd worden via de telefoon en het opnemen van alle gesprekken in een ruimte met behulp van de ingebouwde microfoon.

Wandklok met GSM zender

Micro GPS Tracker

Rookmelder met camera

Pen met opnameapparatuur

Camouflage camera

Opritverklikker

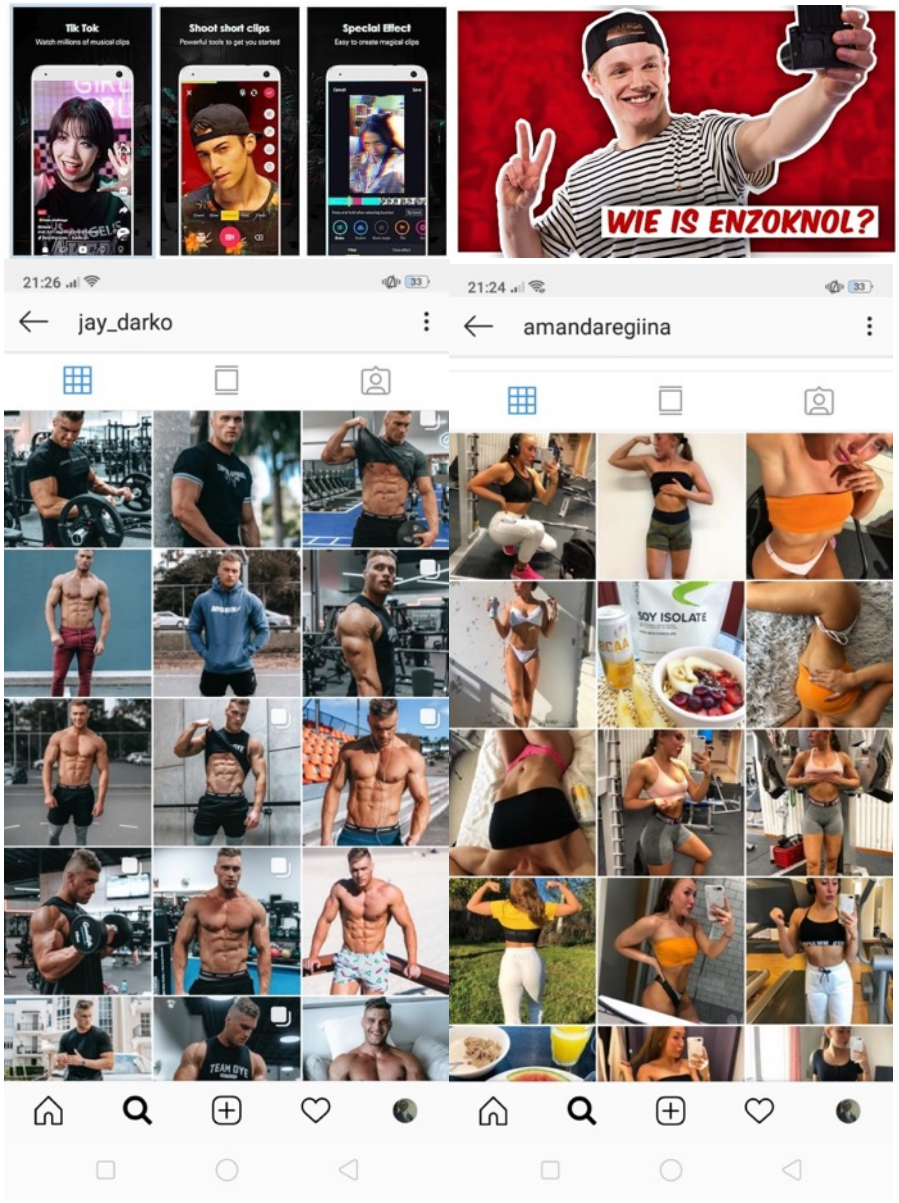
Afbeelding 1: Er zijn talloze winkels en webshops die 'spionage apparatuur' verkopen. Onderstaande voorbeelden en afbeeldingen komen van: https://www.sitcon.nl/. Bij de software gaat het om: https://www.sitcon.nl/samsung-galaxy-note-spy-software.html en https://www.sitcon.nl/spyware/

2.3.4 Informatie-infrastructuur

Naast het aanbod van apparatuur is ook de informatie-infrastructuur waarbinnen de opname en eventuele verspreiding van heimelijk verzamelde informatie geschiedt de afgelopen decennia structureel veranderd. De opnameproducten zelf kunnen steeds langer opnemen zonder dat de batterij of accu moet worden vervangen en de producten maken het mogelijk om de opnames van afstand uit te lezen. Dergelijke opnames kunnen eenvoudig worden verspreid via het internet, of in *real time* worden gestreamd. Technologische of economische barrières om beelden of geluidsopnames openbaar te maken via Youtube, Instagram, Facebook of andere fora zijn er nauwelijks meer.

2.3.5 Online informatiecultuur

Door de beschikbare informatie-infrastructuur is ook een cultuur ontstaan waarin het maken van opnames van jezelf en het delen van deze gegevens met vrienden of de hele wereld de standaard is geworden. Instagram, Tiktok, Facebook en de diverse sites van *vloggers* draaien om het maken van opnames van jezelf, waarbij veelal het idee is dat deze vormen van *self-exposure* leidt tot meer vrienden, roem, of commercieel of artistiek succes. Om op te vallen in de zee aan filmpjes en foto's gaan mensen steeds gekkere dingen doen en steeds intiemere gegevens delen. Door *quantified-self* technieken zijn mensen ook in staat om steeds meer gegevens over zichzelf op te nemen en te delen in online *communities* die datzelfde doen. Dat betekent dat er een steeds grotere hoeveelheid gegevens en intieme informatie door mensen zelf wordt gedeeld, waarmee het steeds makkelijker wordt voor derden om daar misbruik van te maken.



Afbeelding 2: Enkele voorbeelden van de online informatiecultuur. Bronnen: https://nl.ccm.net/download/downloaden-34091789-tik-tok-voor-android; https://www.youtube.com/watch?v=IfI6TTVoV2c; https://thepreviewapp.com/instagram-feed-ideas-fitness/

2.3.6 Vervaging van morele grenzen en normalisering van extreem gedrag

De ontwikkeling van een online informatiecultuur heeft ook geleid tot het verleggen en vervagen van ethische en morele grenzen. In de digitale wereld zijn de traditionele sociale instituties en morele autoriteiten die een rol spelen bij de ontwikkeling van het individuele en maatschappelijke geweten, grotendeels afwezig.[18] Ook de effectiviteit van corrigerende mechanismen (uiteenlopend van groepsdruk tot het strafrecht) is op het internet minder groot. Hierdoor ontstaat er een 'morele mist' waarin

[18] Cocking, D., Van den Hoven, J. (2018), *Evil Online*, Blackwell Wiley

schendingen van grondrechten en extreem gedrag genormaliseerd worden.[19] Ook spelen bepaalde kenmerken van het internet een rol bij het schenden van de privacy. Met name de anonimiteit van internetgebruikers en de afstand tot slachtoffers verlagen de drempel voor het schenden van de privacy van medeburgers.

2.3.7 De rol van producenten, distributeurs en tussenpersonen

Veel van de privacyschendingen in horizontale verhoudingen tussen burgers worden gemedieerd door private partijen, die vaak zijn gevestigd in landen met andere privacystandaarden, zoals de Verenigde Staten of China. Daarbij zijn twee typen intermediairs van belang, die elkaar niet noodzakelijkerwijs wederzijds uitsluiten. Enerzijds gaat het om online diensten en platformen zoals Facebook, Twitter en WhatsApp. Anderzijds gaat het om leveranciers van producten die het verzamelen of verspreiden van gegevens mogelijk maken, zoals *drones*, *spyware* en *self-tracking devices*. Deze partijen spelen op een aantal manieren een belangrijke rol in verband met privacyschendingen in horizontale verhoudingen. Producten worden met name ingezet om gegevens te verzamelen, diensten worden met name ingezet om gegevens te verspreiden.

2.3.8 Inferred data

Tot slot moet worden gewezen op de mogelijkheid om door middel van statistische correlaties voorspellende of probabilistische gegevens af te leiden uit bestaande data-punten (zogenoemde *inferred data*). Een tamelijk simplistisch voorbeeld is een bedrijf dat data heeft over hoe vaak personen Marmite kopen en afreizen naar Groot-Brittannië. Uit deze informatie kan het bedrijf met een bepaalde zekerheid afleiden dat het gaat om personen met een Britse nationaliteit of achtergrond. In realiteit werken *Big Data* processen uiteraard met vele honderden datapunten, die op een zeer complexe manier aan elkaar zijn verbonden en gerelateerd. Door de toegenomen rekenkracht kunnen steeds meer datapunten worden verzameld en aan elkaar worden gekoppeld en kan daar met steeds grotere zekerheid andere informatie uit worden afgeleid.

2.4 Privacygevaren

Uit deze ontwikkelingen volgen een aantal privacygevaren, die deels gelijklopen aan de punten die eerder in dit hoofdstuk aan bod zijn gekomen. Die gevaren zullen in het hiernavolgende hoofdstuk worden gebruikt om de verschillende waarden die hiermee op het spel staan te beschrijven en te duiden vanuit een juridisch perspectief.

2.4.1 Veiligheid

'Slimme apparaten' zijn vaak slecht beveiligd. Zo komt het bijvoorbeeld voor dat digitale beveiligingscamera's zonder medeweten van de burger die ze heeft geïnstalleerd, live beelden uitzenden op het internet. Meer in het algemeen zijn telefoons en computers vaak te hacken, wat derden toegang kan geven tot intieme gegevens. Niet zelden worden zo privéfoto's en video's van bekende personen gestolen met het oog op bijvoorbeeld chantage of economisch gewin.

[19] Ibid.

2.4.2 Vertrouwelijkheid

De vertrouwelijkheid van communicatie komt steeds verder onder druk te staan, omdat communicatie steeds vaker gemedieerd is (denk aan e-mail, telefoon, videobellen en online platforms). Hierdoor hebben de producenten en dienstverleners vaak toegang tot de gegevens (inhoud en/of metadata). Daarbij komt dat de producten en diensten burgers in staat stellen gesprekken en communicatie vaak oneindig lang op te slaan. Zo is het mogelijk om e-mailverkeer van jaren geleden terug te zoeken en maken veel telefoons het mogelijk om alle telefoongesprekken die een persoon voert stelselmatig op te nemen en op te slaan.

2.4.3 Misbruik

Veel van de producten en diensten die horizontale privacyschendingen faciliteren worden gezien als leuke *gadgets* voor hobbyisten. Deze producten en diensten worden doorgaans ook gebruikt voor onschuldige doeleinden, zoals het filmen van een buurtfeest, een verjaardag of de carnavalsoptocht. *Drones* zijn daarvan het voorbeeld *par excellence*.

De meeste producten en diensten kunnen dus zowel worden gebruikt voor legitieme als voor illegitieme doeleinden. Toch is duidelijk dat bepaalde producten met name zijn vervaardigd met het oog op het bevorderen van privacyschendingen in horizontale verhoudingen, zoals kleine camera's die zijn te verstoppen in alledaagse objecten, microfoons in pennen en GPS *trackers* die op auto's kunnen worden geplaatst. Dat geldt ook voor de diensten. Spionage-apps die op de telefoon van een persoon kunnen worden geplaatst om diens telefoongebruik in kaart te brengen, lijken enkel te zijn vervaardigd om de privacy van medeburgers te schenden.

Maar ook rechtmatig verkregen gegevens kunnen worden misbruikt. Bedrijven kunnen de gegevens bijvoorbeeld gebruiken voor commerciële doelen die niet in lijn liggen met het doelbindingsprincipe, of kunnen andere bedrijven toegang tot de data geven voor dubieuze doeleinden. Wanneer gegevens online staan is het moeilijk om het gebruik van die gegevens door andere burgers te controleren; niet zelden zal het dan ook voorkomen dat die gegevens worden misbruikt voor illegale doeleinden. Dat geldt ook als gegevens die met toestemming voor het ene doel (bijvoorbeeld het maken van een privéopname van de liefdesdaad) worden gebruikt voor een ander doel (bijvoorbeeld het toebrengen van reputatieschade aan een ex-partner).

2.4.4 Woning en privésfeer

Producten die op de markt verschijnen staan burgers toe om al dan niet heimelijk beeld of geluid op te nemen, zowel van binnen als van buiten de woning. Infraroodcamera's en geluidssensoren met een groot bereik kunnen door muren heen informatie registreren en drones kunnen worden gebruikt om over iemands heg heen te kijken of door een raam naar binnen. Daarnaast zijn steeds meer apparaten in huis (de slimme meter, de slimme koelkast, de slimme deurbel) verbonden met het internet en verzamelen die gegevens over het privéleven van mensen. Hiermee komt het idee van de woning als afgesloten privéruimte onder druk te staan.

2.4.5 Lichamelijke privacy

Door technologische ontwikkelingen wordt het steeds eenvoudiger om van een afstand in de slaapkamer of de badkamer kijken, sensoren in huizen te plaatsen en opnames te maken op iemands erf. De kans is daarbij groot dat intieme zaken en gedragingen worden bekeken. Dit vormt een aantasting van de lichamelijke privacy. Daarbij moet evenwel worden opgemerkt dat dergelijke intieme beelden ook kunnen worden opgenomen in de publieke en semi-publieke sfeer. Hierbij valt te denken aan verborgen camera's in sauna's en in kleedruimtes van fitnessgelegenheden.

2.4.6 Controle en gedragsverandering

Het feit dat je overal en altijd gefilmd kan worden en dat je daar geen wetenschap van hebt of controle over kunt uitoefenen, kan leiden tot gedragsverandering. Mensen die zich bespied wanen in hun privéomgeving gaan zich anders gedragen, aarzelen om vrienden thuis uit te nodigen, kleden zich kuiser of treffen voorzorgsmaatregelen om opnames te voorkomen. Daarbij komt dat er simpelweg zoveel sensoren zijn dat mensen steeds meer het gevoel kunnen krijgen dat het vechten tegen de bierkaai is om bezwaar te maken tegen opnames of zicht te houden op waar welke gegevens over hen precies zijn opgeslagen en wat er vervolgens gebeurt met die data.

2.4.7 Kennis is macht

Het is van belang te vermelden dat privacyrisico's niet alleen bestaan bij gebruik of misbruik van gegevens. Het enkele feit dat de buurjongen met een drone de privéruimte van de buren heeft waargenomen en de buurvrouw naakt heeft gezien kan als problematisch worden ervaren, ook al was dat niet zijn bedoeling en wist hij de beelden direct. Het verzamelen van informatie over anderen brengt überhaupt een machtsverschuiving met zich mee, omdat een burger meer weet van de ander dan de ander van de een.

2.4.8 Too much information

De producten en diensten kunnen uiteraard ook worden gebruikt voor het verzenden van gevoelige informatie naar mensen die daar niet op zitten te wachten. Zo hebben sommige mannen de neiging om afbeeldingen van hun geslachtsdeel naar vrouwen toe te sturen. Ook dit kan een privacyschending zijn, in de zin dat ongewenste informatie zich jouw leven binnendringt. Ook door informatie op sociale media te zetten kunnen mensen die daar argeloos kennis van nemen aangetast worden in hun persoonlijke levenssfeer.

2.4.9 Cumulatieve privacy-effecten

Tot slot is het van belang dat zelfs als een enkele bron of een enkele opname van een persoon weinig (intieme) informatie blootgeeft, tientallen of honderden verschillende onschuldige informatiebronnen samengenomen een zeer pregnant beeld van iemands (privé)leven kunnen geven. Datzelfde geldt voor de overlast en angst die mensen ervaren. De wetenschap dat er een kleine kans bestaat dat iemand een duur en hooggespecialiseerd product heeft aangeschaft om je te volgen, zoals tot enkele jaren geleden het geval was, is wezenlijk anders dan de wetenschap dat je voortdurend zou kunnen worden bekeken door vrijwel alle medeburgers en bedrijven. Eén keer per jaar een drone over je achtertuin zien vliegen is overkomelijk; gebeurt dat meerdere keren per week dan kan er een permanent gevoel van ongemak en

aantasting in iemands leven sluipen. Daarbij moet uiteraard ook worden opgemerkt dat verschillende datastromen samenkomen en weer worden herverdeeld (via platformen en fabrikanten). Daarmee verdwijnt het zicht op en de controle over de verzamelde data.

3 Waarden en belangen in het geding bij horizontale privacyschendingen

3.1 Introductie

De in het vorige hoofdstuk beschreven handelingen kunnen een impact hebben op de persoonlijke levenssfeer. Met betrekking tot deze impact is het relevant te achterhalen welk belang of waarde in het geding is. Dit stelt ons in staat om een beter beeld te krijgen van de aard en de ernst van de inbreuk. Dit is van belang voor de normering van de inbreukmakende gedraging en eventuele reacties daarop. Door zicht te krijgen op de achterliggende belangen kunnen we ook beoordelen of er lacunes zijn in de normering en de rechtsbescherming. Hierbij moet opgemerkt worden dat de te beschermen belangen doorgaans overlappen en dat de schending van horizontale privacy meerdere belangen kan raken. Zo zullen bijvoorbeeld bij de publicatie van wraakporno de eer en goede naam van het slachtoffer in het geding zijn, maar wordt ook het vertrouwen in intieme relaties ondermijnd.

3.2 Te beschermen belangen en aangetaste waarden (burger-burger)

De onderstaande belangen kunnen worden gezien als deelaspecten of uitwerkingen van het recht op privacy en de menselijke waardigheid. Het betreft hier geen uitputtende lijst. Naar ons oordeel zijn dit evenwel de meest wezenlijke belangen en waarden die in horizontale verhoudingen in het geding kunnen komen.

3.2.1 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).[20] Voorts worden in de clausulering van het recht op vrijheid van meningsuiting (artikel 10 lid 2 EVRM) de eer en de goede naam specifiek als te beschermen belangen genoemd.

Onder 'eer' wordt verstaan de waarde die men in zijn eigen ogen heeft, het gevoel van eigenwaarde. 'Goede naam' doelt op de waarde die men in de ogen van anderen heeft, de reputatie derhalve. Voor aantasting van de goede naam is dus altijd kennisname door derden vereist.[21]

Bij de aantasting van de goede naam gaat het om uitingen die de negatieve beïnvloeding van de (publieke) perceptie van een persoon of organisatie tot doel of gevolg heeft. Maar het kan ook gaan om het gebruik van andermans identiteit, naam of portret zonder de goedkeuring of wetenschap van die persoon. Denk hierbij bijvoorbeeld aan het gebruiken van iemands foto bij een social media post zonder diens toestemming. Ook het toeschrijven van uitspraken aan een persoon die deze niet heeft gedaan tasten de eer en de goede naam aan, bijvoorbeeld omdat zij het beeld van deze persoon vertekenen.[22]

[20] Europees Verdrag voor de Rechten van de Mens, Rome, 4 november 1950, via: https://www.echr.coe.int/Documents/Convention_NLD.pdf
[21] Verheij, A. J. (2002), *Vergoeding van immateriële schade wegens aantasting in de persoon,* Nijmegen: Ars Aequi
[22] Ibid., p. 320

3.2.2 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 (zie 3.2.4), maar het stelt ons ook in staat om selectief te kunnen zijn in het delen van informatie en aspecten van onze persoonlijkheid. Rosen typeert privacy in dit kader als een 'grens' die de persoon beschermt tegen objectivering, simplificering en onterechte beoordeling.[23] Wanneer informatie over een persoon zonder context of toelichting in een andere (sociale) context wordt gebruikt, dan leidt dit al snel tot verkeerde beoordelingen. In zijn boek *the Naked Crowd* beschrijft Rosen dit als volgt:

"It is impossible to know someone on the bases of snippets of information, genuine knowledge is something that can be achieved only slowly, over time, behind a shield of privacy, with the handful of people to whom we've chosen to reveal ourselves whole. And even those who know us best may not know us in all of our complicated dimensions." [24]

Controle over de persoonlijke levenssfeer in het algemeen en persoonlijke informatie in het bijzonder stelt ons in staat om de 'contextuele integriteit' van onze persoon in sociale omgang te behouden.[25]

3.2.3 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. Om die reden speelt het recht op privacy in verticale verhoudingen een belangrijke rol bij het beschermen van de vrijheid van de burger. In horizontale verhoudingen speelt privacy en gegevensbescherming ook een rol bij het behoud van de persoonlijke autonomie, zij het een minder grote rol dan in verticale verhoudingen.

3.2.4 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. In het publieke leven spelen wij allemaal tot op zekere hoogte een sociale rol uit.[26] Het recht op privacy waarborgt een zekere afstand tussen het individu en de buitenwereld. Dit stelt ons in staat om ons 'sociale masker' tijdelijk af te leggen. Het recht op privacy creëert daarmee de ruimte om te experimenteren met onze eigen identiteit en (tijdelijk) te ontkomen aan de druk van sociaal wenselijk of verwacht gedrag. Privacy schept een ruimte om ongedwongen jezelf te kunnen zijn en biedt daarmee de mogelijkheid tot (emotionele) ontlading.[27]

[23] Rosen, J. (2000). *The Unwanted Gaze: the Destruction of Privacy in the United States*, New York: Vintage Books, p. 20
[24] Rosen, J. (2004), *The Naked Crowd*, New York: Random House, p. 161
[25] Nissenbaum, H. (2004), Privacy as contextual integrity, in: *Washington Law Review*, 79(1), 119-157
[26] Goffman, E. (1959), *The Presentation of Self in Everyday Life*, New York: Doubleday, p. 55-57
[27] Westin, A.F. (1967). *Privacy and Freedom*, New York: Atheneum Press, p. 36

3.2.5 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. Je vertelt je beste vriend meer dan een kennis op het werk; je partner vertel je andere dingen dan je vrienden in de kroeg. Daarbij wordt de informatie geacht te blijven binnen de context waarbinnen de persoon die heeft gedeeld.

Het kan zijn dat een relatie van karakter verandert en één van beide partijen andere belangen heeft of ideeën krijgt over de openbaarmaking van gegevens die eerder in vertrouwen zijn gedeeld. Nergens is dit probleem duidelijker dan bij 'wraakporno'. Wanneer binnen een relatie intiem, erotisch materiaal wordt vastgelegd, dan gebeurt dit met wederzijdse toestemming. Doorgaans zullen beide partijen stilzwijgend met elkaar zijn overeengekomen dat deze beelden niet worden gedeeld. Wanneer één van beide partijen dit verbond verbreekt, bijvoorbeeld uit wraak voor een verbroken relatie, dan is er sprake van een horizontale privacyschending. Het wederzijdse vertrouwen wordt dan met terugwerkende kracht geschaad. De wetenschap dat in de toekomst mogelijk beelden of informatie worden gelekt door de ander, of een ervaring waar dit reeds gebeurd is, bemoeilijkt het ontwikkelen van intieme relaties.[28]

Een ander aspect van het recht op privacy dat bij relaties een rol speelt is de zogenaamde *relationele privacy*. Relationele 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. Denk bijvoorbeeld aan een intieme relatie waarvan het bestaan nog niet aan familie of vrienden bekend is gemaakt, of contacten onderhouden met politieke of religieuze groepen. In deze context faciliteert het recht op privacy ook de uitoefening van andere rechten zoals het recht op vergadering en het recht op vrije meningsuiting.

3.2.6 Veiligheid

In de meest extreme vormen kunnen horizontale privacyschendingen ook een bedreiging vormen voor de veiligheid van het slachtoffer of diens gevoel van veiligheid.

Een voorbeeld van een horizontale privacyschending die een bedreiging kan vormen voor de veiligheid is het *doxen* en onvrijwillig *outen* van lhbt'ers.[29] Niet alleen ontneemt een dergelijke schending de persoon in kwestie de mogelijkheid om op eigen voorwaarden met de geaardheid om te gaan en deze bekend te maken, het vormt in bepaalde landen en binnen bepaalde culturen ook een acute bedreiging voor de veiligheid van de betrokkene. Een ander voorbeeld is stalking (belaging). Een belager kan met behulp van allerlei digitale middelen (denk aan locatiebepaling) zijn slachtoffer volgen en vrees aanjagen. Ook pesten krijgt een nieuwe dimensie door digitale middelen. Het fenomeen *cyber-bullying* (cyberpesten) betekent dat zelfs in de beschermde omgeving van het eigen huis, het slachtoffer niet veilig is voor pestkoppen. Cyberpesten is daarmee ook een vorm van horizontale privacyschending.

[28] Keats Citron, D. (2019), *Why sexual privacy matters for trust*, University of Maryland Legal Studies Research Paper No. 2019-02
[29] Doxing' is een neologisme voor het (online) achterhalen van iemands werkelijke identiteit. Wanneer iemand bijvoorbeeld op een forum anoniem communiceert over de seksuele geaardheid en een derde achterhaalt en publiceert de identiteit van deze persoon, dan is er sprake van *doxing*.

3.3 Te beschermen belangen en aangetaste waarden (burger-rechtspersonen)

In de relatie tussen een persoon en een rechtspersoon (een bedrijf, vereniging, stichting enzovoorts) spelen veel van de hierboven genoemde belangen en waarden een rol. Maar specifiek in de relatie tussen personen en rechtspersonen zijn de onderstaande belangen en waarden daarnaast relevant.

3.3.1 Vertrouwelijkheid en controle

Vertrouwelijkheid en controle speelt ook een rol in de relatie tussen personen en rechtspersonen. Wanneer bedrijven bijvoorbeeld persoonsgegevens verzamelen over personen dan verliezen deze personen daar de controle over.[30]

3.3.2 Economische gelijkwaardigheid

In horizontale relaties zijn partijen doorgaans min of meer gelijkwaardig.[31] Echter, wanneer de ene partij veel meer weet over de ander, dan kan dit de gelijkwaardigheid aantasten. 'Informatie asymmetrie' kan allerlei negatieve gevolgen hebben voor de onderliggende partij.[32] Dit vraagstuk speelt met name in de rol tussen natuurlijke personen en bedrijven, omdat het doorgaans de bedrijven zijn die de middelen en het belang hebben om zoveel mogelijk te weten over hun potentiële klanten of medewerkers. 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. Denk hierbij bijvoorbeeld aan prijsdiscriminatie of het *nudgen* van klanten richting bepaalde productgroepen.[33]

3.3.3 Persoonlijke autonomie

De persoonlijke autonomie kan in de relatie tussen burger en bedrijf met name in het geding zijn daar waar het gaat om personeel. Werknemers hebben ook op de werkvloer recht op de bescherming van hun persoonlijke levenssfeer.[34] Wanneer een medewerker op de werkvloer gemonitord wordt door de werkgever dan kan de medewerker zich minder vrij voelen om bijvoorbeeld te communiceren met derden, dit tast de persoonlijke autonomie van de werknemer aan. Hoewel een medewerker in de tijd van de baas wellicht minder 'vrij' is dan in het privéleven rechtvaardigt dit niet vergaande inbreuken op de persoonlijke levenssfeer.

3.3.4 Eer en goede naam

Een belang dat ook in de relatie tussen burgers, bedrijven en andere rechtspersonen in het geding kan komen is de eer en de goede naam. In dit kader kan bijvoorbeeld gedacht worden aan het opstellen van 'zwarte lijsten' van winkeldieven en andere vormen van *naming and shaming* door bedrijven. Verenigingen kunnen in het kader van het handhaven van interne regelementen ook de eer en goede naam van leden

[30] Zie bijvoorbeeld: https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-tennisbond-vanwege-verkoop-van-persoonsgegevens
[31] Dit is ook de reden waarom de bescherming van grondrechten van oorspronkelijk primair haar werking had in verticale verhoudingen.
[32] Akerlof, G. (1970). The market for 'lemons': Quality uncertainty and the market mechanism. In: *The Quarterly Journal of Economics,* 84(3), 488–500.
[33] Thaler, R., Sunnstein, C. (2008), *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Yale University Press
[34] Zie bijvoorbeeld: EHRM 25, juni 1997, app. no. 20605/92 (*Halford v. Verenigd Koninkrijk*), EHRM, 3 april 2007, app. no. 62617/00 (*Copland v. Verenigd Koninkrijk*), EHRM, app. no. 61496/08 (*Barbalescu v. Roemenië*)

aantasten. Wanneer er geen deugdelijk systeem van tuchtrechtspraak is, kan dat leiden tot reputatieschade voor het betrokken lid. Maar burgers kunnen ook de eer en goede naam van rechtspersonen aantasten. Zo kunnen onterechte negatieve uitingen over een bedrijf de reputatie van het bedrijf aantasten.

Tenslotte kunnen de eer en goede naam van personen worden aangetast door hun portret of naam te misbruiken voor commercieel gewin. Een voorbeeld hiervan is het gebruiken van de naam van bekende Nederlanders in malafide Bitcoin advertenties.[35]

3.3.5 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.

3.4 Individu overstijgende waarden

Het verlies van privacy voor een individu kan niet alleen gevolgen hebben voor die persoon zelf, maar ook voor de privacy van anderen.

Allereerst is er een netwerk effect. Als een persoon informatie over zichzelf deelt, dan zegt dat vaak ook iets over de mensen waarmee hij omgaat, zoals zijn partner of, bijvoorbeeld bij medische aangelegenheden, over zijn familieleden. Een klassiek voorbeeld is een foto genomen op een nogal wild feest. Hoewel de centrale figuur op de foto kan instemmen met het plaatsen daarvan op Facebook, zegt de foto ook iets over de anderen aanwezigen (al was het maar dat zij op een wild feest waren).

Daarnaast bestaat een aantal beroepen bij gratie van vertrouwelijkheid. Voor journalisten is het brongeheim wezenlijk; voor advocaten en artsen het beroepsgeheim. Allen stelt in dit verband:

"First, confidentiality encourages seeking medical care. Individuals will be more inclined to seek medical attention if they believe they can do so on a confidential basis. It is reassuring to believe others will not be told without permission that one is unwell or declining, has abused illegal drugs, been unfaithful to one's partner, obtained an abortion, or enlarged one's breasts. […] Second, confidentiality contributes to full and frank disclosures. Individuals seeking care will be more open and honest if they believe the facts and impressions reported to health providers will remain confidential. It may be easier to speak freely about embarrassing symptoms if one believes the content of what one says will not be broadcast to the world at large."[36]

Ook de democratie als zodanig is afhankelijk van vertrouwelijkheid, in het bijzonder de vertrouwelijkheid van het stemhokje.

Andere auteurs benadrukken dat privacy zowel een *common* als een *public good* is. Priscilla Regan schrijft bijvoorbeeld:

[35] Zie: ECLI:NL:RBAMS:2019:8415
[36] Allen, A. L. (2011), *Unpopular privacy. What must we hide?,* Oxford: Oxford University Press, 2011, p. 112.

"Privacy has value beyond its usefulness in helping the individual maintain his or her dignity or develop personal relationships. Most privacy scholars emphasize that the individual is better off if privacy exists; I argue that society is better off as well when privacy exists. I maintain that privacy serves not just individual interests but also common, public, and collective purposes. If privacy became less important to one individual in one particular context, or even to several individuals in several contexts, it would still be important as a value because it serves other crucial functions beyond those that it performs for a particular individual. Even if the individual interests in privacy became less compelling, social interests in privacy might remain. [...] I suggest that three concepts provide bases for discussing a more explicitly social importance for privacy – privacy as a common value, privacy as a public value, and privacy as a collective value. The first two concepts are derived from normative theory, while the latter is derived from economic theory; the styles of analysis, therefore, are different, with the first two being conceptual and the third more technical."[37]

Privacy als publieke waarde is het idee dat privacy niet alleen waardevol is op zichzelf, maar ook instrumenteel is voor andere waarden, zoals de vrijheid van meningsuiting. Het idee van privacy als collectieve waarde is afgeleid van het economische concept van collectieve goederen. Schone lucht en nationale defensie zijn voorbeelden van collectieve goederen. Dat betekent dat zelfs bij privacyschendingen in horizontale verhoudingen, er publieke of collectieve belangen op het spel staan. De schending van de privacy van een flink aantal individuen ontstijgt het individuele niveau: het geheel is groter dan de som der delen.

3.5 Categorisering horizontale privacyvraagstukken

Op grond van het bovenstaande komen wij tot de volgende categorisering van 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*,	Vertrouwelijkheid en controle, vertrouwen in intieme relaties, persoonlijke autonomie, identiteit en

[37] Regan, P.M. (1995), *Legislating Privacy: Technology, Social Values and Public Policy*, Chapel Hill: University of North Carolina Press.

	fake endorsement, doen van niet gedane uitingen, *fake news*	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.

4 Het recht op privacy

In dit hoofdstuk gaan wij in op de ontstaansgeschiedenis en het juridisch kader van het (klassieke) recht op privacy en het recht op bescherming van persoonsgegevens. In dit hoofdstuk geven wij allereerst een toelichting op het recht op privacy in de Nederlandse grondwet. Omdat het recht op privacy in Nederland voornamelijk wordt ingekleurd door EU recht en de jurisprudentie van het EHRM, wordt daar in dit hoofdstuk ook uitgebreid bij stilgestaan.

4.1 Grondwettelijke bescherming van privacy

Het recht op privacy is in de Nederlandse Grondwet vervat in niet minder dan vier verschillende artikelen. Artikel 10 Gw bevat het recht op de persoonlijke levenssfeer en de bescherming van persoonsgegevens, artikel 11 Gw regelt de onaantastbaarheid van het lichaam, artikel 12 Gw beschermt de woning en artikel 13 Gw gaat in op de vertrouwelijkheid van communicatie. Daarin is Nederland zeker niet uniek. Privacy wordt vaak gezien als een koepelrecht, dat bescherming biedt aan diverse aspecten van het leven, waaronder in veel landen ook nog het recht op reputatie en de bescherming van de eer en goede naam vallen. Er is ook een verband tussen privacy en het recht van vergadering en vrijheid van geweten; voor het uitoefenen van deze rechten is immers een bepaalde mate van vertrouwelijkheid vereist, die gewaarborgd kan worden door het recht van privacy.

Ook in andere constituties, zoals bijvoorbeeld in de Duitse en Italiaanse Grondwet, bieden verschillende artikelen bescherming aan de diverse aspecten van het recht op privacy. In internationale verdragen is er juist vaak gekozen voor een samenvoeging van de verschillende onderdelen van dit recht in één artikel, waarbij evenwel moet worden opgemerkt dat de integriteit van het menselijke lichaam vaak ook apart wordt beschermd door verboden op onder meer foltering en dat er vaak ook een apart recht is opgenomen ten aanzien van de vrijheid om te trouwen en een gezin te stichten.

Onderstaand volgt ter illustratie een overzicht van hoe het recht op privacy verschillende verdragen is neergelegd.

Artikel 12 UVRM[38]	**Artikel 8 EVRM**[39]	**Artikel 17 IVBPR**[40]
Niemand zal onderworpen worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of	1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.	1. Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privé leven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam.

[38] Universele Verklaring van de Rechten van de Mens, Parijs, 10 december 1948, via: https://www.un.org/en/universal-declaration-human-rights/
[39] Europees Verdrag voor de Rechten van de Mens, Rome, 4 november 1950, via: https://www.echr.coe.int/Documents/Convention_NLD.pdf
[40] Internationaal Verdrag inzake burgerrechten en politieke rechten, New York, 16 december 1966, via: https://wetten.overheid.nl/BWBV0001017/1979-03-11#Verdrag_2

goede naam. Tegen een dergelijke inmenging of aantasting heeft eenieder recht op bescherming door de wet.	2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.	2. Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting.

Tabel 4.1 Privacybepalingen uit internationale verdragen

Het eerste lid van artikel 10 van de Nederlandse Grondwet heeft nauwelijks een zelfstandige rol van betekenis gespeeld, gezien het belang van artikel 8 EVRM en het gegevensbeschermingsrecht van de EU.[41] Aan het tweede en derde lid is voornamelijk uitvoering gegeven in de kaders van het EU recht. Met het uitdijende bereik van artikel 8 EVRM en de proactieve houding van de EU in het kader van de gegevensbescherming is het waarschijnlijk dat het belang van artikel 10 Gw nog verder naar de achtergrond zal verdwijnen. Wel zijn er pogingen en voorstellen gedaan om het artikel te moderniseren.

Wellicht het belangrijkste voorstel is gedaan in 2010 in het Rapport van de Staatscommissie Grondwet.[42] Daarin werd een voorstel gedaan om het artikel in twee aparte artikelen te splitsen, in navolging van het Handvest.[43] De Staatscommissie meende onder andere dat door een aparte grondwetsbepaling te wijden aan de bescherming van persoonsgegevens duidelijker tot uitdrukking zou komen dat de bescherming van persoonsgegevens niet alleen is gekoppeld aan de bescherming van de persoonlijke levenssfeer, maar ook aan andere grondrechten, zoals de vrije meningsuiting en het discriminatieverbod. Ook meende de Staatscommissie dat het belang van het verwerken van persoonsgegevens de afgelopen jaren al flink was gestegen en vermoedelijk in de toekomst alleen maar groter zou worden. Ze wees daarbij zowel op de technologische ontwikkelingen als op de Europese samenwerking en de globalisering, waardoor de omvang van de uitwisseling en verwerking van persoonsgegevens is gegroeid. In het licht hiervan geeft

[41] Van der Pot, 'Handboek van het Nederlandse staatsrecht', vijftiende druk, p. 390-191; Kortmann, Constitutioneel recht, 4e druk, Kluwer, p. 429.
[42] Staatscommissie Grondwet (2010), *Rapport Staatscommissie Grondwet*, via: https://zoek.officielebekendmakingen.nl/blg-86969.pdf
[43] Ibid.

een verzelfstandiging van het recht op bescherming van persoonsgegevens volgens de Staatscommissie uitdrukking aan de toegenomen betekenis van de verwerking van persoonsgegevens en de wenselijkheid van een behoorlijke bescherming in de huidige samenleving.[44] Over de formulering van het nieuw in te voegen artikel aangaande gegevensbescherming bestond een meningsverschil. In tabel 4.2 staan de drie verschillende voorstellen. Die verschillen zijn relevant in het kader van dit onderzoek omdat één van de mogelijke uitkomsten zou kunnen zijn dat de grondwet ten aanzien van het recht op privacy zou kunnen worden aangevuld, herzien of vernieuwd.

Voorstel Staatscommissie nieuw artikel 10 Gw	**Meerderheidsvoorstel nieuw in te voegen artikel**	**Minderheidsvoorstel nieuw in te voegen artikel**
Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.	1. Ieder heeft recht op bescherming van zijn persoonsgegevens. 2. Persoonsgegevens worden alleen verwerkt voor welbepaalde doeleinden, a. hetzij met toestemming van de betrokkene, b. hetzij op grond van bij de wet te stellen regels. 3. Ieder heeft recht op inzage in de over hem verzamelde gegevens, op kennisneming van de verwerking van die gegevens, en op de verbetering van die gegevens, behoudens bij de wet gestelde beperkingen.	1. Eenieder heeft recht op bescherming van zijn persoonsgegevens. 2. De verwerking van persoonsgegevens wordt geregeld bij en krachtens de wet. 3. De wet stelt regels inzake de rechten van betrokkenen op kennisneming en verbetering van over hen vastgelegde gegevens, alsmede over hun aanspraak op kennisneming van de verwerking hiervan

Tabel 4.2 De verschillende voorstellen voor een nieuw grondwetsartikel.

Omdat de Grondwet vervolgens niet is aangepast naar aanleiding van deze voorstellen en omdat het grondwettelijk recht op privacy, zoals gezegd, weinig betekenis heeft gehad in de praktijk en jurisprudentie, gaan wij met name in op de totstandkomingsgeschiedenis van artikel 10 van de Grondwet. Alhoewel niet alles één op één kan worden vertaald naar beleidsrelevante conclusies, wordt hiermee wel een beeld verkregen van de achtergrond en betekenis van dit recht, hetgeen helpt bij een begrip van de huidige grondwettelijke bepaling, de keuzes die daaraan ten grondslag lagen en de horizontale werking van het grondrecht te duiden.

4.2 Ontstaansgeschiedenis artikel 10 Grondwet

Wat betreft de Nederlandse Grondwet zijn er voorlopers te vinden voor de artikelen 11, 12 en 13 in de teksten van de Grondwet van voor 1983. Deze relatieve continuïteit geldt echter niet voor artikel 10 Gw. Dat artikel is nieuw toegevoegd in 1983. Interessant is dat het recht weliswaar was opgenomen in het uiteindelijke voorstel van de Staatscommissie Cals/Donner, maar dat het niet was ondergebracht in het hoofdstuk met klassieke grondrechten, maar in het hoofdstuk van de sociale grondrechten. De Commissie

[44] Ibid.

stelde in haar verslag dat de technische en maatschappelijke ontwikkelingen het vraagstuk van de persoonlijke levenssfeer (de privacy) klemmend hadden gemaakt. Omdat de Commissie verwachtte dat de technische middelen de sociale afstanden in de toekomst nog meer zouden verkleinen, zou de wetgever daar regels voor moeten treffen. Een reden om deze bepaling als sociaal en niet als klassiek grondrecht te zien is dat klassieke grondrechten werden geacht geen derdenwerking te hebben.[45] Het ging de Commissie er dus specifiek om de horizontale verhoudingen en de positieve plicht van de overheid om burgers te beschermen tegen privacyinbreuken door derden.

Daarnaast besloot de Staatscommissie Cals/Donner om naast de bescherming van de persoonlijke levenssfeer geen specifieke bepaling over de verwerking van persoonsgegevens toe te voegen. De Commissie wees erop dat voor wat betreft onder meer de werkgever-werknemer relatie, regelingen in het privaatrecht zouden kunnen worden opgenomen, en dat voor wat betreft de verwerking van persoonsgegevens door de overheid, naar het administratief recht zou kunnen worden gekeken. *"De toepassing zowel bij de voorbereiding als de uitvoering van administratieve beslissingen op een wijze welke aan die aanspraken recht doet wedervaren, kan beschouwd worden als een uitvloeisel van beginselen van behoorlijk bestuur als fair play, de eis van voldoende voorbereiding van beslissingen en het inachtneming van de eis van overlegging van stukken enz."*[46] Mede omdat het nog onduidelijk was hoe de technische ontwikkelingen zouden verlopen en welke impact zij zouden hebben op de samenleving, achtte de meerderheid van de commissie het wenselijk om een wat algemenere bepaling in de grondwet op te nemen. Een minderheid van de commissie achtte dit te passief en te afwachtend.

In het eerste voorstel van de regering ten aanzien van een nieuwe grondwet, wat betreft het hoofdstuk van de klassieke grondrechten, was in navolging van de Staatscommissie geen algemeen recht aangaande de bescherming van de persoonlijke levenssfeer opgenomen. De regering merkte in de Memorie van Toelichting op dat zij zich aansloot bij het onderscheid tussen sociale en klassieke grondrechten, zoals voorgesteld door de Staatscommissie:

"De klassieke grondrechten vestigen primair een onthoudingsplicht van de overheid; de sociale grondrechten hebben in het algemeen de strekking de overheid tot het treffen van voorzieningen te verplichten. In dit onderscheid hebben de ondergetekenden de rechtvaardiging gevonden een grondwetsherziening op het stuk van de klassieke grondrechten los van de sociale grondrechten aan te vatten. Ook van de overige constitutionele onderwerpen staan de klassieke grondrechten los, in zoverre, dat zij afzonderlijk te behandelen zijn zonder dat geprejudicieerd wordt op andere grondwetsbepalingen."[47]

Daarom is het des te interessanter dat in een volgende versie van de grondwetsherziening de regering wel een apart privacyartikel heeft toegevoegd en wel aan de lijst met klassieke grondrechten en niet aan die met sociale grondrechten, zoals de Staatscommissie voorstelde:

[45] Cals, J.M.L.Th., Donner, A. M. (1971), Eindrapport van de Staatscommissie van Advies inzake de Grondwet en de Kieswet', Den Haag, Staatsuitgeverij, via: http://resources.huygens.knaw.nl/watermarker/pdf/cc/scans/1967a_cie_cals-donner/verslag/plenair/data/1971-03-29/1971-03-29.pdf

[46] Ibid., p. 238

[47] Tweede Kamer, zitting 1970-1971, 11 051, nr. 3

"Dit vindt bevestiging in het directe verband met het huisrecht en het briefgeheim, welke steeds als klassieke grondrechten zijn beschouwd (…). Wij staan op het standpunt, dat het probleem van de doorwerking van de grondrechten in de horizontale verhoudingen geen bezwaar oplevert de bescherming van de persoonlijke levenssfeer als een direct werkend recht te redigeren." [48]

Omdat het recht op bescherming van de persoonlijke levenssfeer algemener en onbepaalder werd bevonden, is ervoor gekozen om deze bepaling vóór het recht op de bescherming van de woning en vertrouwelijkheid van communicatie te plaatsen.

Daarnaast besluit de regering ook, tegen het voorstel van de Staatscommissie in, om een lid te wijden aan de bescherming van persoonsgegevens. Daarbij meent de regering dat het aanleggen en gebruiken van registraties van persoonsgegevens zeer ingrijpende gevolgen voor de persoonlijke levenssfeer kan hebben. *"Dit leidt ons tot de mening, dat niet moet worden volstaan met een algemeen geredigeerde privacybepaling doch dat een opdracht aan de wetgever om op het terrein van het vastleggen van persoonsgegevens regelend op te treden op zijn plaats is. Deze gedachte is neergelegd in het tweede lid"*[49] Belangrijk is dat de regering benadrukte dat dit lid niet alleen betrekking heeft op door de overheid vastgelegde persoonsgegevens. Ten aanzien van derde lid volgt de regering de mening van de minderheid van de Staatscommissie, die meende dat een bepaling aangaande transparantie niet in de grondwet mocht ontbreken:

"Wij gaan daarbij nog wat verder door deze opdracht ook te doen gelden voor de kennisneming van het gebruik, dat van de vastgelegde gegevens wordt gemaakt. Dit gebruik immers kan, zoals hierboven en in de toelichting op het eerste lid is aangegeven, van betekenis zijn voor de vraag of iemands persoonlijke levenssfeer is aangetast."[50]

De Raad van State, in zijn advies over het wetsvoorstel, raadde af om de leden twee en drie in de Grondwet op te nemen:

"Het gaat hier om de verdere uitwerking van het geformuleerde essentiële beginsel, welke verdere uitwerking aan de wetgever kan worden overgelaten. Wanneer in de memorie van toelichting onder de te beschermen privésfeer mede worden opgesomd de abonnementen en lidmaatschappen, evenals sommige gewoonten, gedragingen en contacten, dan valt er nog heel wat in nadere regelen te vatten. Daarbij moet bovendien worden overwogen, dat het recht op inzage en verbetering van alle zodanige persoonlijke gegevens eveneens duidt op een uitgebreid en gecompliceerd wetgevingsprogramma. Een aanzet voor dit programma in de Grondwet zelf is niet nodig, omdat de Grondwet geen inhoudsopgave van de gewone wetgeving is."[51]

[48] Tweede kamer, zitting 1975-1976,13 872, nr. 3
[49] Tweede Kamer, zitting 1975-1976,13 872, nr. 3
[50] Tweede Kamer, zitting 1975-1976,13 872, nr. 3
[51] Tweede Kamer, zitting 1975-1976,13 872, nr. 4

In de daaropvolgende kamerdiscussie was er met name veel aarzeling ten aanzien van lid 3 van het voorgestelde artikel 10 Gw. De leden behorende tot de fracties van de KVP, de ARP en de CHU vroegen zich bijvoorbeeld af waarom het derde lid aan dit artikel is toegevoegd en het derde lid kwam ook de leden van de PvdA-fractie te mager voor. Uit de VVD-fractie kwam het verzoek om motieven te noemen voor beperking van het inzagerecht en de leden van de C.P.N.-fractie zetten 'hele grote vraagtekens' bij de betekenis van het derde lid.[52]

In de Memorie van Antwoord stelt de regering dat door het schappen van lid 3, er een verarming van het grondrecht zou optreden:

"Dat deze punten toch wel uit de formulering van het tweede lid zouden voortvloeien achten wij minder vanzelfsprekend dan [de leden van de fracties van K.V.P., A.R.P. en C.H.U]. Aan de andere kant lijkt ons de suggestie van de leden van de P.v.d.A.-fractie het derde lid om te zetten in een direct werkend recht te ver te gaan. Er is op het terrein van de persoonsregistratie nog veel onbekend; er moet nog veel terreinverkenning plaatsvinden. Voor dat nog niet geïnventariseerde gebied thans reeds een grondwettelijk en in rechte afdwingbaar inzage-en correctierecht in te voeren komt ons prematuur voor. Wij wijzen er ook op, dat het tweede en derde lid in de voorgestelde redactie ook op de horizontale verhoudingen betrekking hebben. Ten aanzien van een direct werkend inzage- en correctierecht zou het bezwaarlijk zijn aanstonds horizontale werking te aanvaarden. Wij menen met de opdracht in het derde lid, die wij niet gaarne zouden missen, toch de meest adequate grondwettelijke voorzieningen te hebben geboden die op dit terrein thans kunnen worden gegeven. Het derde lid bevat een opdracht aan de wetgever, geen direct werkend recht. Er kan derhalve geen sprake zijn van enige beperking van dit recht, noch van motieven tot een zodanige beperking, zoals door de leden van de V.V.D. worden gevraagd."[53]

Wel worden er in de Nota van Wijzigingen aanpassingen gedaan door de regering:

"De leden van de fracties van K.V.P., A.R.P. en C.H.U. bepleiten deze opdracht uit te breiden met het verwerken en verstrekken van persoonsgegevens. Wij hebben in de memorie van antwoord opgemerkt, dat dit inhoudelijk aan onze bedoeling beantwoordt en dat een aanvulling van het voorgestelde artikel in deze geest ook naar onze mening een verbetering zou zijn. Dit geldt vooral voor het verstrekken. Een uitdrukkelijke toevoeging van het verwerken ligt naar onze mening minder voor de hand, aangezien dit verwerken gewoonlijk een technisch administratieve aangelegenheid is en daar, waar het uit een oogpunt van bescherming van de persoonlijke levenssfeer relevant wordt, reeds tot het vastleggen of het verstrekken kan worden gerekend. Het gaat er bij artikel 1.10 immers om welke gegevens worden vastgelegd en wat er daarna mee gebeurt, dat wil zeggen aan wie ze worden doorgegeven. Dit lijkt ons met «vastleggen en verstrekken» voldoende gedekt. Op grond hiervan stellen wij voor in artikel 1.10 lid 2 aan het vastleggen het verstrekken toe te voegen."[54]

[52] Tweede Kamer, zitting 1975-1976,13 872, nr. 6

[53] Tweede Kamer, zitting 1975-1976,13 872, nr. 7

[54] Tweede Kamer, zitting 1976-1977,13 872, nr. 8

Uit deze korte bespreking van de totstandkomingsgeschiedenis van artikel 10 Gw volgen drie punten. Ten eerste blijkt dat het algemene privacy- en gegevensbeschermingsrecht altijd al was voorzien als zijnde gedeeltelijk of grotendeels relevant voor horizontale verhoudingen. Ten tweede blijkt dat er als gevolg daarvan er aanvankelijk voor werd gekozen om het algemene privacy- en gegevensbeschermingsrecht als sociaal grondrecht te behandelen. Sociale grondrechten, zoals de bevordering van de volksgezondheid (artikel 22 Gw) of de bevordering van voldoende werkgelegenheid (artikel 19 Gw), zijn in tegenstelling tot klassieke grondrechten (zoals het recht op vrijheid van meningsuiting of vrijheid van religie) geen subjectieve klachtrechten. Uiteindelijk is er echter voor gekozen om het algemene privacy- en gegevensbeschermingsrecht toch in de lijst met klassieke grondrechten op te nemen. Ten derde en tot slot was met name tegen leden twee en drie van artikel 10 Gw, waarin het recht op gegevensbescherming en het recht op informatie over de verwerking van gegevens en de correctie van foutieve gegevens is vervat, verzet van zowel de Raad van State als van een aantal Kamerfracties. Kern van deze kritiek was dat deze rechten te vergaand zouden zijn en een te breed toepassingsbereik zouden hebben. Toch heeft de regering er voor gekozen deze, toentertijd vooruitstrevende en controversiële bepalingen op te nemen, met het oog op toekomstige technologische ontwikkelingen.

4.3 Het recht op persoonlijke levenssfeer onder het EVRM

Artikel 10 Gw biedt bescherming aan twee rechten: de bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens, waaronder het recht op inzage en correctie. Bij beide rechten is de waarde van het artikel in de Nederlandse Grondwet beperkt. Ten aanzien van de persoonlijke levenssfeer is de jurisprudentie van het Europees Hof voor de Rechten van de Mens met betrekking tot artikel 8 van het EVRM dominant. Ten aanzien van het recht op bescherming van persoonsgegevens is de Europese Unie leidend, met jurisprudentie van het Europees Hof van Justitie met betrekking tot onder meer artikel 8 uit het Handvest en de regelgeving zoals vervat in de Algemene verordening gegevensbescherming (AVG). Hieronder staan wij stil bij de bescherming van de persoonlijke levenssfeer, in de volgende paragraaf bij het recht op gegevensbescherming.

Net zoals alle mensenrechten is het recht op privacy niet onbeperkt. Mensenrechten werken met een dubbele conditionaliteit. Ten eerste zijn er voorwaarden voor de toepasbaarheid van het recht in kwestie en ten tweede zijn er voorwaarden waaronder, als aan alle voorwaarden voor de toepasbaarheid van een recht is voldaan, het recht in kwestie kan worden beperkt. In deze paragraaf zal bij twee van de voorwaarden voor de toepasbaarheid worden stilgestaan, namelijk de *ratione personae* (persoonlijke reikwijdte) en de *ratione materiae* (materiële reikwijdte*).* De eerste ziet op de vraag of de persoon in kwestie (onder het EVRM kan een klacht alleen worden ingediend tegen een staat die is aangesloten bij de Raad van Europa) inderdaad een klachtrecht toekomt. Normaliter komt de buurman van een persoon waar een huiszoeking is gepleegd bijvoorbeeld geen klachtrecht toe. Het tweede principe ziet op de vraag of de inhoud van de klacht wel onder de materiële reikwijdte van het recht valt. Na de behandeling van deze twee principes zal nog kort worden stilgestaan bij de beperkingssystematiek van artikel 8 EVRM.

4.3.1 Persoonlijke reikwijdte

Het EVRM kent twee soorten klachten: (1) klachten tussen staten (bijvoorbeeld Noorwegen start een zaak tegen Zweden wegens schending van mensenrechten) en (2) individuele klachten. Het individuele

klachtrecht staat open voor drie soorten klagers: (2a) natuurlijke personen, (2b) niet-gouvernementele organisaties en (2c) groepen natuurlijke personen. Klachten kunnen alleen tegen staten worden ingediend. De focus lag oorspronkelijk op klachten tussen staten, aangezien het EVRM werd opgesteld tegen de achtergrond van de Tweede Wereldoorlog. De kern van de Conventie was aanvankelijk niet het beschermen van specifieke belangen van individuele eisers, maar om groot en systematisch machtsmisbruik door staten te voorkomen.

Het toezicht op de Conventie bestond uit twee niveaus. Allereerst besloot de Europese Commissie voor de Rechten van de Mens (ECMHR), die nu niet meer bestaat, over de ontvankelijkheid van zaken. Alleen ten aanzien van de Commissie bestond het mechanisme van individuele klachten. Zelfs als een zaak ontvankelijk was verklaard door de Commissie, had de individuele klager (natuurlijke persoon, rechtspersoon of groep) niet het recht om de zaak voor te leggen aan het Europees Hof voor de Rechten van de Mens (EHRM), die een inhoudelijk oordeel over de zaak velde. Een zaak kon alleen aan het Hof worden voorgelegd door de Commissie of door een lidstaat die was aangesloten bij de Raad van Europa. Het idee was dat alleen individuele klachten die betrekking hadden op of raakten aan een algemeen belang, aan het EHRM zou worden voorgelegd ter beoordeling.

Deze keuze van de verdragsopstellers is in de loop der tijd radicaal omgedraaid, wat juist ook goed te zien is ten aanzien van het recht op privacy. Het Hof stelt dat in principe alleen natuurlijke personen een klacht kunnen indienen aangaande het recht op privacy. In het algemeen komen interstatelijke klachten, waarbij bijvoorbeeld Nederland een klacht indient tegen Oostenrijk over een schending van één of meer rechten onder het Verdrag, nauwelijks voor. Ook heeft het EHRM geoordeeld dat alleen personen die elk individueel zijn geraakt door een zelfde inbreuk hun klachten kunnen bundelen. In tegenstelling tot andere rechten, zoals de vrijheid van meningsuiting en de vrijheid van religie waar het Hof wel bereid is om naar de klachten van rechtspersonen te kijken, kunnen rechtspersonen in principe geen beroep doen op artikel 8 EVRM. Rechtspersonen hebben geen privéleven, zo stelt het Hof.

"[T]he extent to which a non-governmental organization can invoke such a right must be determined in the light of the specific nature of this right. It is true that under Article 9 of the Convention a church is capable of possessing and exercising the right to freedom of religion in its own capacity as a representative of its members and the entire functioning of churches depends on respect for this right. However, unlike Article 9, Article 8 of the Convention has more an individual than a collective character (…)."[55]

Dat betekent dat in de praktijk vrijwel alleen natuurlijke personen een klacht kunnen indienen over een mogelijke schending van artikel 8 EVRM. Daarbij komt dat het Hof vereist dat deze personen concrete en daadwerkelijke schade hebben ondervonden van een concrete en specifieke inbreuk. Kan dat niet worden aangetoond, dan worden hun klachten niet-ontvankelijk verklaard. Zogenoemde *in abstracto* klachten, die gaan over een wet of beleid als zodanig, zonder dat de eisers beweren daar zelf hinder van te hebben ondervonden, worden in principe niet-ontvankelijk verklaard.[56] Ook zogenoemde *a-priori* klachten, waarin een zaak wordt aangebracht nog voordat de privacy-inbreuk zich heeft voltrokken, worden in principe niet-

[55] ECmHR, Church of Scientology of Paris v. France, application no. 19509/92, 09 January 1995.
[56] EHRM, 14 juli 1988, app. no. 12763/87 (*Lawlor v. The United Kingdom*)

ontvankelijk verklaard.[57] Ook geldt er de zogenoemde *de minimis* regel, dat vereist dat de klager niet alleen een causaal verband tussen het doen en nalaten van de staat en de geleden schaden moet aantonen, maar dat het ook om substantiële schade moet gaan: "*The Court shall declare inadmissible any individual application [] if it considers that [] the applicant has not suffered a significant disadvantage.*"[58]

In dit verband kan worden opgemerkt dat de subjectieve beleving van het slachtoffer nauwelijks een rol van betekenis speelt. Alhoewel het EHRM de term *'reasonable expectation of privacy'* in een handvol zaken (voornamelijk tegen het Verenigd Koninkrijk) gebruikt, speelt deze doctrine geen grote rol van betekenis. Dit is anders in bijvoorbeeld het Verenigd Koninkrijk, waar wordt gewerkt met de doctrine van 'reasonable expectation of privacy', of, *"if there is room for doubt whether information is private, if disclosure of the information about the individual concerned would give substantial offence to a person of ordinary sensibilities placed in similar circumstances to that individual."* Kinderen genieten onder deze doctrine een grotere bescherming dan volwassenen.

In principe worden zaken derhalve alleen ontvankelijk verklaard als er concrete en daadwerkelijke schade aan het individu is toegebracht door een concrete en specifieke inbreuk door de staat. Dat betekent ook dat hypothetische klachten, over een inbreuk waarvan de klager niet zeker weet of die zich heeft voorgedaan, niet-ontvankelijk worden verklaard, en dat het EHRM geen zaken in behandeling neemt waarin de klagers niet opkomen voor hun eigen belang, maar voor de belangen van anderen of de samenleving in haar geheel. Ook deze zogenoemde algemeen belangacties of groepsvorderingen, *class actions* of *actio popularis*, worden in principe niet-ontvankelijk verklaard.[59] Tot slot is het EVRM zo gewijzigd dat individuele klagers wiens klacht ontvankelijk is verklaard hun zaak zelf kunnen voorleggen aan het Hof voor een inhoudelijke beoordeling.

Kortom, er is door het EHRM een zeer grote nadruk gelegd op de persoonlijke belangen van de natuurlijke persoon als het gaat om klachten ten aanzien van artikel 8 EVRM. De laatste tijd is daar wel enige versoepeling in opgetreden. Zo is het Hof is bereid geweest om een twintigtal klachten van rechtspersonen met betrekking tot artikel 8 EVRM toe te staan, onder meer wanneer hun bedrijfsruimten werden doorzocht door politiefunctionarissen zonder een gerechtelijk bevel.[60] Ook is het EHRM sinds kort geneigd om groepsbelangen van minderheden te beschermen, al komen groepen als groep nog geen klachtrecht toe. Tot slot heeft het Hof in 2015 geoordeeld dat in uitzonderlijke gevallen zogenoemde *in abstracto* klachten, over de wet of beleid als zodanig, ontvankelijk kunnen worden verklaard.[61]

4.3.2 Materiële reikwijdte

De materiële reikwijdte van artikel 8 EVRM is sinds de jaren '50 van de vorige eeuw flink uitgebreid. Aanvankelijk was het bedoeld als negatief en verticaal afweerrecht, dat primair negatieve verplichtingen voor de staat met zich bracht. Net zoals binnen de Nederlandse context een verschuiving naar positieve

[57] ECmHR, 4 december 1995, app. no. 28204/95 (*Tauira and others v. Frankrijk*).
[58] Artikel 35 EVRM.
[59] EHRM, 29 juni 1999, app. no. 29121/95 (*Asselbourg and 78 others and Greenpeace Association-Luxembourg v. Luxemburg*)
[60] van der Sloot, B. (2015), Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system', in: *The Computer Law & Security Review*, 2015-1, p. 26-45.
[61] EHRM, 4 december 2015, app. no. 47143/06 (*Roman Zakharov v. Rusland*)

plichten van de staat en bescherming van privacy in horizontale verhoudingen is waar te nemen heeft ook het EHRM, met de *living instrument* doctrine in de hand, de reikwijdte van het recht op privacy stelselmatig uitgebreid. Artikel 8 EVRM biedt niet langer alleen bescherming aan negatieve rechten voor burgers, het omvat volgens het EHRM ook veel positieve rechten; het vereist niet alleen dat staten zich onthouden van misbruik van hun bevoegdheden, maar ook dat zij hun bevoegdheden gebruiken om de burger actief te beschermen.

Meer in het algemeen biedt artikel 8 EVRM, en dan in het bijzonder het begrip 'privéleven', bescherming aan vrijwel alles dat enigszins raakt aan persoonlijke belangen en de persoonlijke ontwikkeling van een individu. Ook aan de andere drie elementen van artikel 8 EVRM, de bescherming van het familieleven, de woning en de correspondentie, is door het EHRM een ruime reikwijdte toegekend. Bovendien heeft het recht op privacy andere rechten die in het EVRM zijn vervat in meer of mindere mate opgeslokt. Ook wordt naar artikel 8 EVRM verwezen om belangen te beschermen die expliciet uit het Verdrag zijn geweerd door de verdragsopstellers en wordt artikel 8 EVRM gebruikt om nieuwe rechten te beschermen.

Hieronder zal daarvan een aantal voorbeelden worden gegeven waaruit blijkt dat vrijwel alles wat direct of indirect raakt aan iemand persoonlijke ontwikkeling of levenskwaliteit, onder artikel 8 EVRM kan vallen. Alhoewel niet al deze specifieke voorbeelden direct relevant zijn voor privacyschendingen in horizontale verhoudingen geven ze wel een indruk van de reikwijdte van het recht. Ook laat het zien dat het recht in een aantal decennia een enorme groei en verandering heeft doorgemaakt. Daaruit lijkt te volgen dat als het EHRM dat met het oog op maatschappelijke en technologische ontwikkelingen in de toekomst opportuun acht, het waarschijnlijk niet zal aarzelen om nieuwe waarden of rechten onder de paraplu van het recht op privacy te scharen.

4.3.2.1 Privéleven

Hoewel het recht op bescherming van het privéleven oorspronkelijk was beperkt tot persoonlijke zaken in het privédomein, biedt het momenteel bescherming aan bijna elk aspect van iemands leven. Zo valt onder de bescherming van het privéleven onder meer de persoonlijke ontwikkeling van een individu, toegang tot onderwijs, de ontwikkeling van sociale relaties, privacy in het publieke domein en het biedt in bepaalde gevallen zelfs bescherming tegen ontslag, omdat het EHRM van mening is dat werk belangrijk is voor de persoonlijke ontwikkeling van een mens. Onder omstandigheden geeft artikel 8 EVRM ook een recht op toegang tot overheidsinformatie, zodat een individu beredeneerde beslissingen over zijn/haar leven kan nemen.[62]

4.3.2.2 Gezinsleven

Alhoewel het begrip gezinsleven oorspronkelijk alleen werd toegepast op de traditionele familie, heeft het EHRM dit begrip in de loop van de tijd behoorlijk uitgebreid. Ook relaties met tantes, neven, grootouders, broers en zussen, schoonfamilie en stieffamilie kunnen hier onder vallen, wat ook geldt voor de relatie tussen een kind en zijn wettelijke vertegenwoordiger of voogd. De bescherming van het familieleven uit artikel 8 EVRM biedt niet alleen bescherming tegen onrechtmatige inbreuken door de staat (bijvoorbeeld

[62] Zie: van der Sloot, B. (2017), *Decisional privacy 2.0: the procedural requirements implicit in Article 8 ECHR and its potential impact on profiling*, in: *International Data Privacy Law*, Volume 7, Issue 3, 1 August 2017

het uit huis plaatsen van een kind), maar ook de positieve vrijheid om dergelijke relaties aan te gaan en te laten opbloeien. Erkenning van het omgangsrecht met de biologische ouder is een mooi vroeg voorbeeld van werking van artikel 8 EVRM in horizontale relaties. Het gezinsleven kan op velerlei wijzen door digitale ontwikkelingen onder druk komen te staan. Een voorbeeld hiervan is dat digitale apparaten het seksleven van partners registreren of dat geliefden apps gebruiken om inschattingen te maken en advies te geven over hun vruchtbaarheid, het al dan niet gezonde verloop van de zwangerschap en de gezondheid van het opgroeiende kind.[63]

4.3.2.3 Woning

Hoewel het Europees Hof voor de Rechten van de Mens in zijn vroege jurisprudentie een vrij traditionele benadering koos ten aanzien van wat onder het begrip 'woning' kon worden verstaan, valt in de huidige interpretatie van het EHRM vrijwel elk object waar een persoon woont, leeft of anderszins aan is verbonden daaronder. Het EHRM biedt zelfs bescherming aan schuren, bedrijfsruimtes en openbare gebouwen, met een verwijzing naar dit begrip: zo kan het feit dat de politie een hoofdkantoor binnentreedt om stukken in beslag te nemen onder omstandigheden worden gezien als een inbreuk op het huisrecht van dat bedrijf.[64] Het is duidelijk dat ook het huisrecht onder druk komt te staan door digitale ontwikkelingen, onder meer door het feit dat het huis steeds meer wordt bevolkt door producten die in constante verbinding met het internet staan en daarmee informatie over het huishouden doorgeven aan derden. Denk hierbij bijvorbeeld aan de slimme koelkast, de slimme meter, de slimme deurbel, slimme sekspeeltjes en slim kinderspeelgoed.

4.3.2.4 Correspondentie

Correspondentie geniet ook bescherming onder artikel 8 EVRM. Onder het begrip correspondentie worden niet alleen meer traditionele vormen van communicatie verstaan, maar ook correspondentie door middel van moderne technieken, zoals het internet. Ook biedt het EHRM bescherming tegen de interceptie van metadata – de gegevens over de communicatie. Aangezien vrijwel alle communicatie gemedieerd plaatsvindt (via e-mail, Skype, WhatsApp, et cetera) is er een steeds grotere hoeveelheid gegevens die niet meer onder de directe controle van de burger valt. Hierdoor wordt de kans groter dat derden zoals bedrijven die advertenties aanbieden aan de hand van de inhoud van online gesprekken, of inlichtingendiensten die infiltreren in groepen en netwerken, inzicht krijgen in deze gegevens.

4.3.2.5 Het recht op een eerlijk proces

Het recht op een eerlijk proces wordt beschermd krachtens artikel 5 en met name artikel 6 EVRM. Hoewel deze bepalingen nog steeds zeer invloedrijk zijn en de meeste zaken onder het EVRM betrekking hebben op artikel 6 EVRM, is het toch zo dat wanneer kwesties van behoorlijke procesgang, procedurele waarborgen en een eerlijk proces verband houden met privacyaangelegenheden, het EHRM bereid is dergelijke elementen onder het recht op privacy zelf te bespreken:

[63] Zie bijvoorbeeld: https://www.cosmopolitan.com/sex-love/a17887712/best-pregnancy-tracker-app/
[64] Zie voor het eerst: EHRM, 16 april 2002, app. no. 37971/97 (*Stes Colas est e.a. v. Frankrijk*). Zie verder: van der Sloot, B. (2015), Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system, in: *The Computer Law & Security Review*, 2015-1, p. 26-45

"Article 8 contains no explicit procedural requirements, but this is not conclusive of the matter. The local authority's decision-making process clearly cannot be devoid of influence on the substance of the decision, notably by ensuring that it is based on the relevant considerations and is not one-sided and, hence, neither is nor appears to be arbitrary. Accordingly, the Court is entitled to have regard to that process to determine whether it has been conducted in a manner that, in all the circumstances, is fair and affords due respect to the interests protected by Article 8."[65]

Aangezien steeds meer besluitvormingsprocessen worden geautomatiseerd en door middel van algoritmische processen worden afgehandeld zal ook dit aspect van het recht op privacy steeds belangrijker worden in de 21ste eeuw.

4.3.2.6 De bescherming van de reputatie

Artikel 8 EVRM is gebaseerd op artikel 12 UVRM, dat ook bescherming biedt aan de reputatie, de eer en goede naam, naast de bescherming van privé- en gezinsleven, de woning en communicatie. De bescherming van reputatie werd door de opstellers van het EVRM expliciet uitgesloten van de werkingssfeer van artikel 8 EVRM en is verplaatst naar artikel 10, tweede lid, EVRM. Een van de redenen was dat het recht op reputatie met name ook in horizontale verhoudingen een rol speelt, terwijl het EVRM was bedoeld voor verticale verhoudingen. Lid 2 van artikel 10 EVRM bevat het recht op vrijheid van meningsuiting en voorziet in de voorwaarden voor beperking van dit recht. Bijgevolg was de bescherming van de reputatie niet bedoeld als een subjectief recht van burgers, maar als een grond op basis waarvan regeringen de vrijheid van meningsuiting mogen (en niet moeten) beperken. Hoewel het EHRM deze principiële keuze lang heeft gerespecteerd, is hier sinds 2009 verandering in gekomen, toen het expliciet heeft bepaald dat de bescherming van de reputatie, eer en goede naam wel een subjectief recht is onder het EVRM, namelijk als onderdeel van het recht op privacy.[66]

In het Verenigd Koninkrijk zijn in de rechtspraak criteria ontwikkeld om de vrijheid van meningsuiting te wegen tegen het recht op privacy en de bescherming van de reputatie (meer specifiek met betrekking tot het fotograferen van personen in de publieke ruimte).[67] Het gaat dan om:

- the attributes of the claimant;
- the activity in which the claimant was engaged;
- the location;
- the nature and purpose of the intrusion;

---

[65] Zie: EHRM, 8 juli 1987, B, app. no. 9840/82 (*B v. Verenigd Koninkrijk*). Zie verder: EHRM, 3 april 2012, app. no. 42857/05 (*Van der Heijden v. Nederland*), EHRM 21 februari 1975, app. No. 4451/70, (*Golder v. Verenigd Koninkrijk*), EHRM 16 december 1992, app. no. 13710/88 (*Niemitz v. Duitsland*)

[66] Zie over dit onderwerp: EHRM, 11 maart 1985, app. no. 10733/84 (*Asociacion de Aviadores de la Republica, Mata et al. v. Spanje*); EHRM, 24 augustus 1999, app. no. 31135/96 (*Saltuk v. Turkije*); EHRM, 5 december 2000, app. no. 42015/98 (*Marlow v. het Verenigd Koninkrijk*); EHRM, 15 januari 1997, app. no. 31477/96 (*Rayayd and Unanua v. Spanje*); EHRM, 14 juni 2005, app. no. 14991/02 (*Minelli v. Zwitserland)*; EHRM, 17 oktober 2006, app. no. 71678/01 (*GourGuénidzé v. Georgië*); EHRM, 24 juni 2004, app. no. 59320/00 (*Von Hannover v. Duitsland*); EHRM, 16 november 1986, app. no. 11366/85 (*N. v. Zweden*); EHRM, 10 oktober 2006, app. no. 7508/02 (*L. L. v. Frankrijk*); EHRM, 15 november 2007, app. no. 12556/03 (*Pfeifer v. Oostenrijk*); EHRM, 4 december 2012, app. no. 6490/07 (*Rothe v. Oostenrijk*); EHRM, 9 april 2009, app. no. 28070/06 (*A. v. Noorwegen*)

[67] *Murray v Big Pictures* [2008] EWCA Civ 446

- consent;
- the effect on the claimant;
- circumstances in which the publisher obtained the information.

4.3.2.7 Lichamelijke en psychologische integriteit

Ook het recht op lichamelijke integriteit, dat niet expliciet wordt genoemd in artikel 8 EVRM, maar in artikel 2 (het recht op leven) en artikel 3 (het verbod op foltering), wordt deels beschermd via het recht op privacy. Artikelen 2 en 3 hebben, net zoals artikel 12 EVRM, een beperkte materiële reikwijdte gekregen, terwijl artikel 8 EVRM juist een zeer ruime reikwijdte is toegekend. Bijgevolg wordt ten aanzien van vraagstukken rond medische procedures, verplichte vaccinatie, abortus, euthanasie en andere medisch-ethische vraagstukken met name verwezen naar het recht op privacy.[68] Ook het lichaam wordt door middel van digitale technieken steeds meer onder druk gezet. Zo kunnen er door middel van gezichtsherkenningstechnologieën emoties van mensen worden gedetecteerd. Keymolen *et al.* stellen in dit kader:

"Emotiedetectie als een specifieke vorm van gezichtsherkenning kan ook een rol spelen in beveiliging en controle, bijvoorbeeld wanneer bepaalde emoties als angst en boosheid op geautomatiseerde wijze herkend worden en dit wordt gebruikt om snel op te treden en escalatie te voorkomen. (…) Zeker de mogelijkheid om met emotiedetectie, een specifieke vorm van gezichtsherkenning, geautomatiseerd en real-time te kunnen monitoren hoe klanten zich voelen en daar dan proactief op in te kunnen spelen, is een toepassing die commerciële partijen als veelbelovend beschouwen. Nieuwe functionaliteiten die gepersonaliseerde dienstverlening of advertenties nog verder verfijnen, zoals het meten van de hartslag op basis van digitale videobeelden van gezichten, maken het automatisch analyseren van gezichten nog aantrekkelijker. Als deze tendens zich voortzet, dan is het mogelijk dat door middel van gezichtsherkenning data real-time worden gekoppeld aan individuen in de (semi)publieke ruimte met het doel hun handelen te beïnvloeden (ook wel nudging genoemd) of hen te profileren. Niemand krijgt dan nog dezelfde aanbiedingen te zien in winkels en er kan op geautomatiseerde wijze onderscheid gemaakt worden in de manier waarop mensen worden behandeld. Gezichtsherkenning wordt dan een belangrijke sleutel om data-gedreven beslissingen te nemen en de keuze-infrastructuur van burgers in het dagelijks leven te beïnvloeden."[69]

---

[68] EHRM, 10 december 1984, app. no. 10435/83 (*Acmanne a.o. v. België*); EHRM, 12 juli 1978, app. no. 7154/75 (*Association of parents v. het Verenigd Koninkrijk*); EHRM, 2 december 1985, app. no. 10787/84 (*Wain v. het Verenigd Koninkrijk*); EHRM, 10 december 1975, app. no. 6907/75 (*X. v. Denemarken*); EHRM, 4 februari 1982, app. no. 8542/79 (*Godfrey v. het Verenigd Koninkrijk*); EHRM, 16 juni 2005, app. no. 61603/00 (*Storck v. Duitsland*); EHRM, 22 juli 2003, app. no. 24209/94 (*Y.F. v. Turkije*); EHRM, 27 augustus 1992, app. no. 12850/87 (*Tomasi v. Frankrijk*); EHRM, 5 mei 1981, app. no. 8509/79 (*X. v. Duitsland*); EHRM, 13 november 2006, app. no. 36150/03 (*Benito v. Spanje*); EHRM, 25 maart 1993, app. no. 13134/87 (*Costello-Roberts v. het Verenigd Koninkrijk*); EHRM, 7 mei 1981, app. no. 8334/78 (*X. v. Duitsland*); EHRM, 22 februari 1995, app. no. 20872/92 (*A.B. v. Zwitserland*); EHRM, 9 september 1998, app. no. 34199/96 (*Galloway v. het Verenigd Koninkrijk*); EHRM, 6 april 1994, app. no. 21132/93 (*Peters v. Nederland*); EHRM, 4 december 1978, app. no. 8239/78 (*X. v. Nederland*); EHRM, 13 december 1979, app. no. 8278/78 (*X. v. Oostenrijk*), Acmanne (n 84); EHRM, 29 april 2002, app. no. 2346/02 (*Pretty v. het Verenigd Koninkrijk*); EHRM, 19 mei 1976, app. no. 6959/75 (*Brüggemann and Scheuten v. Duitsland*); EHRM, 26 mei 2011, app. no. 27617/04 (*R.R. v. Polen*); EHRM, 14 mei 2002, app. no. 38621/97 (*Zehnalova and Zehnal v. Tsjechië*) ; EHRM, 4 januari 2005, app. no. 14462/03 (*Pentiacova and 48 others v. Moldavië*)

[69] Keymolen, E., *et al.* (2020), *Op het eerste gezicht: Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties*, WODC projectnummer 2992, p. 9

4.3.2.8 Eigendomsrecht

Het eigendomsrecht werd uitdrukkelijk uit het EVRM geweerd en naar het Eerste Protocol verwezen, onder meer omdat het EVRM zou gaan om eerste generatie mensenrechten (klassiek politieke afweerrechten) en niet om tweede generatie mensenrechten (sociaaleconomische rechten, ten aanzien waarvan van de staat juist actie wordt gevraagd). Verder werden verscheidene voorstellen om in artikel 8 van het EVRM de bescherming van privé-eigendom op te nemen verworpen. Toch heeft het EHRM deze keuze al vanaf het begin tenietgedaan en consequent bescherming geboden aan privé-eigendom met een verwijzing naar artikel 8 EVRM, zoals wanneer het ging om erfvraagstukken, vernietiging van eigendommen en huizen en het recht te werken.[70] Uiteraard is het recht op eigendom relevant in de digitale omgeving, al wel het maar omdat er een voortdurende discussie is over de vraag of burgers een eigendomsrecht op een data zouden moeten hebben.

4.3.2.9 Persoonlijkheidsrechten

Alhoewel de UVRM verschillende bepalingen bevat die bescherming bieden aan iemands persoonlijkheid, werden deze artikelen niet overgenomen in het EVRM, onder meer omdat ze als te vaag en weinig specifiek werden gezien. Momenteel fungeert artikel 8 EVRM echter als een persoonlijkheidsrecht - het biedt bescherming voor bijna elk aspect van het leven, de ontwikkeling en de bloei van een persoon.[71] In toenemende mate staat in de privacyliteratuur de vraag centraal welke invloed de data-gedreven samenleving heeft op de vrije en ongehinderde vorming van individuele persoonlijkheden en identiteiten van met name kinderen en jongvolwassenen.[72]

---

[70] EHRM, 29 maart 2011, app. no. 23445/03 (*Esmukhambetov a.o. v. Rusland*); EHRM, 3 mei 2011, app. no. 1503/02 (*Mzayev a.o. v. Rusland*); EHRM, 15 februari 2007, app. no. 37850/97 (*Aksakal v. Turkije*); EHRM, 29 november 1991, app. no. 12849/87 (*Vermeire v. België*); EHRM, 3 oktober 2000, app. no. 28369/95 (*Bourimi v. Nederland*); EHRM, 24 juli 2003, app. no. 40016/98 (*Karner v. Oosternrijk*); EHRM, 27 juli 2004, app. no. 55480/00 & 59330/00 (*Sidabras and Dziautas v. Litouwen*); EHRM, 24 februari 2005, app. no. 10523/02 (*Coorplan-Jenni GMBH and Hascic v. Oostenrijk*); EHRM, 19 oktober 2010, app. no. 20999/04 (*Ozpinar v. Turkije*); EHRM, 9 januari 2013, app. no. 21722/11 (*Oleksandr Volkov v. Oekraïne*); EHRM, 14 maart 2013, app. no. 24117/08 (*Bernh Larsen Holding AS a.o. v. Noorwegen*)

[71] EHRM, 3 november 2011, app. no. 29770/05 (*Arvelo Apont v. Nederland*); EHRM, 13 juni 1979, app. no. 6833/74 (*Marckx v. België*); EHRM, 18 mei 1976, app. no. 6825/ 74 (*X. v. IJsland*); EHRM, 26 februari 2002, app. no. 36515/97 (*Frette v. Frankrijk*); EHRM, 17 januari 2012, app. no. 20376/05 (*Varapnickaite-Mazyliene v. Litouwen*); EHRM, 25 november 2008, app. no. 23373/03 (*Biriuk v. Litouwen*); EHRM, 25 november 2008, app. no. 36919/02 (*Niene v. Litouwen*); EHRM, 20 december 2007, app. no. 23890/02 (*Phinikaridou v. Cyprus*); EHRM, 7 februari 2002, app. no. 53176/99 (*Mikulic v. Kroatië*); EHRM, 7 juli 1989, app. no. 10454/83 (*Gaskin v. het Verenigd Koninkrijk*); EHRM, 1 september 1993, app. no. 18806/91 (*K.B. v. Nederland*); EHRM, 11 juli 2002, app. no. 28957/95 (*Goodwin v. het Verenigd Koninkrijk*); EHRM, 25 maart 1992, app. no. 13343/87 (*B. v. Frankrijk*); EHRM, 11 juli 2002, app. no. 25680/94 (*I. v. het Verenigd Koninkrijk*); EHRM, 22 oktober 1981, app. no. 7525/76 (*Dudgeon v. het Verenigd Koninkrijk*); EHRM, 17 juli 1986, app. no. 10389/83 (*Johnson v. het Verenigd Koninkrijk*); EHRM, 26 oktober 1988, app. no. 10581/83 (*Norris v. Ierland*); EHRM, 19 mei 1976, app. no. 6959/75 (*Brüggemann and Scheuten v. Duitsland*); EHRM, 18 januari 2001, app. no. 27238/95 (*Chapman v. het Verenigd Koninkrijk*); EHRM, 27 juli 2010, app. no. 41029/04 (*Aksu v. Turkije*); EHRM (Grote Kamer), 15 maart 2012, app. no. 41029/04 (*Aksu v. Turkije*); EHRM, 15 mei 1980, app. no. 8317/78 (*McFeeley v. het Verenigd Koninkrijk*); EHRM, 6 maart 1982, app. no. 8231/78 (*X. v. het Verenigd Koninkrijk*); EHRM, 10 maart 1981, app. no. 8741/79 (*X. v. Duitsland*); EHRM, 30 maart 1989, app. no. 10461/83 (*Chappell v. het Verenigd Koninkrijk*); EHRM, 7 augustus 1996, app. no. 21794/93 (*C. v. België*)

[72] Zie onder andere: WRR, 'Big Data in een vrije en veilige samenleving', WRR-rapport, Amsterdam University Press, Amsterdam 2016. Montreal Declaration <https://www.montrealdeclaration-responsibleai.com/the-declaration>; Hamer, J., Kool, L. (red.) (2018), *Beschaafde Bits – Zeventien experts over fatsoenlijk digitaliseren*. Den Haag: Rathenau Instituut

4.3.2.10 Het recht op gegevensbescherming

Alhoewel het EVRM geen verwijzing naar een recht op gegevensbescherming bevat, biedt het EHRM aan vrijwel alle aspecten van dit recht bescherming met een verwijzing naar artikel 8 EVRM.[73] Wel geldt er alleen bescherming voor gegevens als die aan iemands privéleven raken.

4.3.2.11 Het recht op een schone en gezonde leefomgeving

Hoewel het EHRM nog niet een recht op leven in een schone en gezonde leefomgeving als zodanig aanvaardt, is het wel degelijk bereid om daar aan gerelateerde zaken te behandelen met een verwijzing naar artikel 8 EVRM. Voorbeelden zijn onder meer kwesties die draaien om geluidshinder, luchtvervuiling, geurvervuiling en andere vormen van milieuschade. Voorwaarde is dat de vervuiling de 'kwaliteit van leven' van de klager moet aantasten (waarbij het EHRM toegeeft dat dat een zeer vaag en subjectief begrip is).[74] Ook dit recht werkt in horizontale verhoudingen: zo hebben burgers met succes geklaagd over de geluidsoverlast veroorzaakt door vliegvelden.[75] Burgers op toeristische plekken, zoals Kinderdijk, klagen momenteel ook over de geluids- en omgevingsoverlast die de vrijwel continu vliegende drones van toeristen veroorzaken. Of het EHRM zal oordelen dat dit voldoende hinder veroorzaakt om onder het recht op de bescherming van het privéleven te vallen is momenteel onzeker, maar uitgesloten is het zeker niet.

4.3.3 Beperkingen

Uit het bovenstaande blijkt dat het recht op privacy en de notie van het privéleven en de persoonlijke levenssfeer zeer breed geïnterpreteerd worden. Dat betekent uiteraard niet dat dit recht ongelimiteerd geldt. Het tweede lid van artikel 8 EVRM bepaalt:

"Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."

Een inperking van het recht op privacy wordt geacht in overeenstemming te zijn met het EVRM wanneer aan drie cumulatieve vereisten is voldaan: (1) de inbreuk moet een wettelijke basis hebben; (2) moet één

[73] EHRM, 25 september 2001, app. no. 44787/98 (*P.G. and J.H. v. het Verenigd Koninkrijk*); EHRM, 17 juli 2003, app. no. 63737/00 (*Perry v. het Verenigd Koninkrijk*); EHRM, 6 september 1978, app. no. 5029/71 (*Klass a.o. v. Duitsland*); EHRM, 2 augustus 1984, app. no. 8691/79 (*Malone v. het Verenigd Koninkrijk*); EHRM, 26 maart 1987, app. no. 9248/81 (*Leander v. Zweden*); EHRM, 5 oktober 2010, app. no. 420/07 (*Köpke v. Duitsland*); EHRM, 3 april 2007, app. no. 62617/00 (*Copland v. het Verenigd Koninkrijk*); EHRM, 25 juni 1997, app. no. 20605/92 (*Halford v. het Verenigd Koninkrijk*); EHRM, 28 januari 2003, app. no. 4467/98 (*Peck v. het Verenigd Koninkrijk*); EHRM, 16 februari 2000, app. no. 27798/95 (*Amann v. Zwitserland*); EHRM, 4 mei 2000, app. no. 28341/95 (*Rotaru v. Roemenië*); EHRM, 2 september 2010, app. no. 35623/05 (*Uzun v. Duitsland*); EHRM, 23 oktober 2012, app. no. 22373/04 (*Hadzhiev v. Bulgarije*)

[74] EHRM, 16 juli 1986, app. no. 9310/81 (*Rayner v. het Verenigd Koninkrijk*), EHRM, 17 mei 1990, app no .13728/88 (*Spire v. Frankrijk*); EHRM, 16 november 2004, app. no 4143/02 (*Moreno Gomez v. Spanje*); EHRM, 14 november 2000, app. no 36735/97 (Villa v. Italië); EHRM, 22 mei 2003, app. no. 41666/98 (*Kyrtatos v. Griekenland*); EHRM, 6 september 2005, app no. 75287/01 (*Morcuende v. Spanje*); EHRM, 17 januari 2006, app. no. 42756/02 (*Luginbuhl v. Zwitserland*); EHRM, 9 december 1994, app. no. 16798/90 (*López Ostra v. Spanje*); EHRM, 10 februari 2011, app no 30499/03 (*Dubetska a.o. v. Oekraïne*); EHRM, 9 juni 2005, app. no. 55723/00 (*Fadeyeva v. Rusland*); EHRM, 26 oktober 20006, app. nos 53157/99, 53247/99, 56850/00 and 53695/00 (*Ledyayeva, Dobrokhotova, Zolotareva and Romashina v. Rusland*).

[75] EHRM, 8 juli 2003, app. no. 36022/97 (*Hatton e.a. v. het Verenigd Koninkrijk*)

van de legitieme doelen dienen die worden genoemd in het tweede lid van artikel 8 EVRM; en (3) noodzakelijk zijn in een democratische samenleving. Wij bespreken deze vereisten kort, aangezien het hier gaat om beperkingen door de staat in verticale verhoudingen. Geen van de drie vereisten zijn direct van toepassing in horizontale verhoudingen.

Het EHRM oordeelt dat een inperking op artikel 8 EVRM niet is voorgeschreven bij wet als aan één of meerdere van de volgende punten niet is voldaan.

In de eerste plaats wordt een schending van het verdrag geconstateerd als de acties van overheidsfunctionarissen niet gebaseerd zijn op een wettelijke bepaling die hen die bevoegdheid verleent. Ten tweede wordt een overtreding vastgesteld als de voorwaarden zoals gespecificeerd in de wet voor het gebruik van bepaalde bevoegdheden niet zijn nageleefd, bijvoorbeeld als politieambtenaren geen rechterlijk bevel hebben om het huis van een burger te betreden. Ten derde moet de wet zelf toegankelijk zijn en begrijpelijk.

In de loop der tijd heeft het Hof een andere voorwaarde gekoppeld aan het criterium van een wettelijke grondslag, namelijk de 'kwaliteit van de wet'. Dit criterium speelt met name een rol ten aanzien van het recht op privacy. Het Hof vereist dat er in de wetgeving regels zijn opgenomen die arbitraire machtsinzet voorkomen en toezicht op machtsinzet mogelijk maken. Zo heeft het Hof onder meer geoordeeld:

"*Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.*"[76]

De nadruk ligt hier dus op rechtsstatelijke aspecten en de *rule of law*, het al dan niet toekennen van '*unfettered power*' aan overheidsinstanties en het bestaan van waarborgen tegen '*arbitrary interference*'. Dit '*quality of law*'-criterium brengt mee dat een wet: (1) helder moet beschrijven welke bevoegdheden er worden toegekend, (2) onder welke voorwaarden deze kunnen worden ingezet, (3) welke parlementaire en rechterlijke controle er geldt voor de inzet van deze bevoegdheden en (4) welke middelen de burger toekomen om eventueel machtsmisbruik te voorkomen.[77]

Het Hof kan ook een schending van artikel 8 EVRM vaststellen als de inbreuk geen legitiem doel dient. De tweede alinea specificeert een aantal legitieme doelen, voornamelijk met betrekking tot veiligheidsgerelateerde aspecten, zoals nationale veiligheid, openbare veiligheid en de preventie van criminaliteit. Het recht op privacy kan ook op legitieme wijze worden beperkt om de rechten en vrijheden van derden te beschermen; een kind kan bijvoorbeeld buitenshuis worden geplaatst (een inbreuk op het recht op gezinsleven van de ouders), omdat de ouders het kind hebben misbruikt. De bescherming van

[76] EHRM, 2 augustus 1984, app. no. 8691/79 (*Malone v. het Verenigd Koninkrijk*)
[77] Zie onder andere: EHRM, 4 december 2015, app. no. 47143/06 (*Roman Zakharov v. Rusland*)

gezondheid en goede zeden kan worden ingeroepen om het recht op privacy te beperken, hoewel deze categorie terughoudend wordt toegepast door het EHRM, omdat de bescherming van de moraal van een land tot vrij beperkende regels kan leiden. Toch kan deze grondslag worden ingeroepen met betrekking tot controversiële medische of seksuele kwesties, zoals euthanasie of BDSM. Ten slotte kan een staat een beroep doen op het 'economisch welzijn van het land'. Deze grond is alleen te vinden in artikel 8 EVRM, geen enkele andere bepaling van het verdrag noemt het economisch welzijn van het land. Het wordt in een aantal gevallen door landen gebruikt; als een aanvrager bijvoorbeeld klaagt over het feit dat een fabriek of luchthaven in de buurt van haar huis haar recht op privéleven schendt. De staat kan dan stellen dat het goede functioneren van een nationale luchthaven noodzakelijk is voor het economische welzijn van het land.

Er kan veel meer worden gezegd over het gebruik, de omvang en de interpretatie van de legitieme doelen, maar dit is niet nodig, omdat dit vereiste geen grote rol van betekenis speelt. Dit komt door twee factoren. Ten eerste is het EHRM vaak niet specifiek over welke term precies van toepassing is, en benadrukt het dat een inbreuk "duidelijk een legitiem doel" was, of dat "onbetwist is dat de inbreuk een van de doelen diende zoals vervat in artikel 8 EVRM". Het combineert verder vaak categorieën, waarbij wordt onderstreept dat de inbreuk een legitiem doel diende, zoals 'de preventie van criminaliteit', 'het economisch welzijn van het land' of 'de rechten van anderen' of het geeft alleen een lijst van alle verschillende doelen en is van mening dat een van deze gronden van toepassing is in het onderhavige geval. Bovendien introduceert het nieuwe doelstellingen, die niet zijn opgenomen in artikel 8 EVRM, met name in zaken die draaien om positieve verplichtingen voor staten. Ten tweede vindt het Hof op dit punt bijna nooit een schending van artikel 8 EVRM. Het geeft de overheid meestal een zeer ruime beoordelingsmarge met betrekking tot de vraag of en welke van de doelstellingen van toepassing zijn in een specifiek geval en of de inbreuk daadwerkelijk dat doel diende. In veel gevallen negeert het dit vereiste gewoonweg bij het analyseren van een mogelijke schending van het recht op privacy of neemt het deze op in de vraag of de inbreuk noodzakelijk was in een democratische samenleving.

Dat dwingt evenwel niet tot de conclusie dat het Hof deze eis geringschat. Een oordeel over het tweede vereiste krijgt met name betekenis binnen de proportionaliteitstoets, die onder het derde vereiste plaatsvindt. Het derde vereiste is dat de inbreuk noodzakelijk moet zijn in een democratische samenleving. Het EHRM heeft in zijn jurisprudentie de vraag naar noodzakelijkheid vervangen door een zogenoemde balancing test. [78] Om de uitkomst van een zaak te bepalen, weegt het EHRM de schade die een specifieke privacy-inbreuk heeft toegebracht aan de individuele persoon af tegen het voordeel ten aanzien van het publieke belang dat met deze inbreuk is gemoeid.

4.4 Afsluitende beschouwing

In dit hoofdstuk zijn twee zaken aan bod gekomen. De grondwettelijke bescherming van privacy en de bescherming van het recht op privacy door het Europees Verdrag voor de Rechten van de Mens.

[78] Rainey, B., Wicks, E., Ovey, C, (2002), Jacobs, White and Ovey: The European Convention on Human Rights, Seventh Edition, p. 209.

Ten aanzien van de Nederlandse Grondwet is besproken dat de relevantie van de privacybescherming die deze wet biedt, gezien het toetsingsverbod en het grote belang van met name de jurisprudentie van het Europees Hof voor de Rechten van de Mens op dit punt, beperkt is. Toch is een belangrijke waarde van het grondwettelijke neerleggen van kernprincipes de signaalfunctie die daarvan uitgaat en het feit dat het parlement wetsvoorstellen aan de grondwet dient te toetsen.

Het recht op privacy is in de Nederlandse Grondwet vervat in niet minder dan vier verschillende artikelen. Artikel 10 Gw bevat het recht op de persoonlijke levenssfeer en de bescherming van persoonsgegevens, artikel 11 Gw regelt de onaantastbaarheid van het lichaam, artikel 12 Gw beschermt de woning en artikel 13 Gw gaat in op de vertrouwelijkheid van communicatie. De rechten uit artikel 11, 12 en 13 zijn in de loop der decennia slechts in beperkte mate gewijzigd en geüpdatet. Artikel 10 Gw is nieuw ingevoegd tijdens de grondwetsherziening van 1983; pogingen om het artikel nadien aan te passen zijn gestrand. Dit artikel leent zich als inspiratiebron en startpunt voor eventuele verdere herzieningen van de Nederlandse Grondwet ten behoeve van privacybescherming in de 21ste eeuw. Uit de korte schets van de totstandkomingsgeschiedenis van artikel 10 Gw volgen drie punten. Ten eerste bleek dat het algemene privacy- en gegevensbeschermingsrecht altijd al was voorzien als zijnde gedeeltelijk of grotendeels relevant voor horizontale verhoudingen. Ten tweede bleek dat als gevolg daarvan er aanvankelijk voor werd gekozen om het algemene privacy- en gegevensbeschermingsrecht als sociaal grondrecht te behandelen. Uiteindelijk is er echter voor gekozen om het algemene privacy- en gegevensbeschermingsrecht toch in de lijst met klassieke grondrechten op te nemen. Ten derde en tot slot was met name tegen leden twee en drie van artikel 10 Gw, waarin het recht op gegevensbescherming en het recht op informatie over de verwerking van gegevens en de correctie van foutieve gegevens is vervat, verzet van zowel de Raad van State als van een aantal Kamerfracties. Kern van deze kritiek was dat deze rechten te vergaand zouden zijn en een te breed toepassingsbereik zouden hebben. Toch heeft de regering ervoor gekozen deze, toentertijd vooruitstrevende en controversiële bepalingen op te nemen, met het oog op toekomstige technologische ontwikkelingen.

Uit de bespreking van de jurisprudentie van het Europees Hof voor de Rechten van de Mens ten aanzien van artikel 8 EVRM, bleek kort gezegd dat het Hof bereid is geweest dit artikel te herinterpreteren al naar gelang het tijdsbeeld, de maatschappelijke of de technische ontwikkelingen daartoe noopten. Van een vrij beperkt afweerrecht is het recht op privacy uitgegroeid tot een 'moederrecht' dat bij uitstek biedt aan kernwaardes als persoonlijke autonomie, menselijke waardigheid, zelfontplooiing en vrijheidsbeleving. Het biedt al de nodige bescherming tegen privacyinbreuken door middel van nieuwe technieken en applicaties en het ligt in de lijn der verwachtingen dat het Hof het artikel nog verder zal aanpassen en herinterpreteren als het dat noodzakelijk acht met het oog op verdere technologische ontwikkelingen.

5 De horizontale werking van grondrechten

In dit hoofdstuk richten wij ons op de vraag in hoeverre het recht op privacy als grondrecht doorwerkt in horizontale verhoudingen.

5.1 Privacy als element van de menselijke waardigheid

Het recht op privacy en gegevensbescherming hangt nauw samen met de menselijke waardigheid. In de Universele Verklaring van de Rechten van de Mens worden in de preambule de menselijke waardigheid en het hebben van grondrechten nadrukkelijk met elkaar verbonden:

"Overwegende, dat erkenning van de inherente waardigheid en van de gelijke en onvervreemdbare rechten van alle leden van de mensengemeenschap grondslag is voor de vrijheid, gerechtigheid en vrede in de wereld."[79]

De menselijke waardigheid vormt als het ware de basis en de ratio voor het hebben van grondrechten.[80] Zo wordt in de preambule van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten erkend dat de rechten opgenomen in het verdrag *"voortvloeien uit de inherente waardigheid van de menselijke persoon"*.[81]

De menselijke waardigheid vereist dus dat ieder mens onvervreemdbare grondrechten heeft, waaronder het recht op privacy en gegevensbescherming. De vraag is echter in hoeverre deze rechten bescherming bieden in horizontale verhoudingen en in hoeverre zij op basis van verdrag of grondwet daadwerkelijk afdwingbaar zijn.

De klassieke grondrechten zoals deze zijn vastgelegd in internationale verdragen en in de constituties van landen zijn primair gericht op het beschermen van de burger tegen de staat.[82] Grondrechten hebben hun gelding daarmee primair in de verticale relatie tussen de staat en haar onderdanen. De belangrijkste gedachte hierbij is dat er sprake is van een ongelijke machtsverhouding waarbij de staat de bovenliggende partij is.[83] Grondrechten zijn noodzakelijk om de macht van de staat ten opzichte van haar onderdanen te begrenzen en te controleren. In horizontale verhoudingen (tussen burgers en organisaties onderling) is er doorgaans geen sprake van een dergelijke scheve machtsverhouding. Partijen zijn min of meer gelijkwaardig en daarmee lijkt er geen noodzaak te zijn voor klassieke grondrechten in deze relaties. Eventuele geschillen kunnen binnen het privaatrecht worden afgedaan.

---

[79] Universele Verklaring van de Rechten van de Mens, Parijs, 10 december 1948, via: https://www.un.org/en/universal-declaration-human-rights/

[80] Zie in dit kader onder andere de Universele Verklaring van de Rechten van de Mens, Het Internationaal Verdrag inzake Burgerechten en Politieke Rechten, het Europees Verdrag voor de Rechten van de Mens en het Handvest voor de grondrechten van de Europese Unie.

[81] Internationaal Verdrag inzake Burgerrechten en Politieke Rechten, New York, 16 december 1966, via: https://wetten.overheid.nl/BWBV0001017/1979-03-11#Verdrag_2

[82] Voor de sociale grondrechten geldt dat deze rechten een opdracht voor de staat inhouden om deze rechten voor de onderdanen te verwezenlijken.

[83] Gerards, J. (2019), *General principles of the European Convention on Human Rights*, p. 135

Toch blijkt het dat mensenrechten ook in horizontale verhoudingen geschonden worden en dat burgers aanspraak maken op de bescherming van hun menselijke waardigheid ten opzichte van andere burgers en bedrijven. Hierdoor is een behoefte ontstaan om de grondrechten die in grondwetten en verdragen hun werking hebben in verticale relaties, ook door te laten werken in horizontale relaties.

5.2 Bescherming van de privacy via de horizontale werking van grondrechten.

5.2.1 Horizontale werking van grondrechten in de nationale rechtsorde

In de loop der tijd is in de grondrechtelijke doctrine de horizontale werking van grondrechten steeds verder doorgedrongen. De horizontale werking van grondrechten (ook wel *derdenwerking* genoemd) houdt in dat personen zich niet enkel tegen de staat op hun grondrechten kunnen beroepen, maar ook deze rechten in kunnen roepen tegen andere personen en organisaties.

5.2.1.1 Duitsland

Hoewel in diverse landen discussie werd gevoerd over de horizontale werking van grondrechten, is de erkenning door het Duitse *Bundesverfassungsgericht* (BVerfGE) in 1954 van de toepasselijkheid van artikel 1 van de Duitse grondwet in private verhoudingen een belangrijk moment voor de erkenning van de horizontale werking van grondrechten geweest.[84] Het Hof stelde in het *Schacht/Leserbriefen* arrest dat artikel 1 van de Duitse Grondwet, dat de onaantastbaarheid van de menselijke waarde beschermt, ook in private verhoudingen ingeroepen kan worden. Het BVerfGE overwoog:

"Nachdem nunmehr das Grundgesetz das Recht des Menschen auf Achtung seiner Würde (Art 1 GrundG) und das Recht auf freie Entfaltung seiner Persönlichkeit auch als privates, von jedermann zu achtendes Recht anerkennt, soweit dieses Recht nicht die Rechte anderer verletzt oder gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt (Art 2 GrundG), muß das allgemeine Persönlichkeitsrecht als ein verfassungsmäßig gewährleistetes Grundrecht angesehen werden [...]"[85]

De menselijke waardigheid (die door het eerste artikel van de Duitse Grondwet wordt beschermd) dient te worden beschermd tegen eenieder. Als zodanig kan het recht op respect voor deze waardigheid dan ook tegen eenieder worden ingeroepen. Uit deze conclusie leidt het Hof een 'algemeen persoonlijkheidsrecht' af dat ook in private verhoudingen zijn gelding heeft.

In het *Lüth* arrest werd de horizontale werking van grondrechten bevestigd.[86] het BVerfGE gaf aan dat de Duitse Grondwet uitstraalt naar alle andere wetgeving en aldus ook het privaatrecht beïnvloedt.[87] Dit betekent dat de civiele rechter bij het wegen van de belangen van partijen ook nadrukkelijk de constitutionele rechten van partijen moet meewegen, ook al gaat het om een geschil in horizontale verhoudingen.[88]

[84] De Vos, B. J. (2010), *Horizontale werking van grondrechten. Een kritiek,* Universiteit Leiden
[85] BVerfG 25 mei 1954, BGHZ 13, 334. (Schacht / Leserbriefentscheid)
[86] BVerfG, 15 januari 1958, 1 BvR 400/51. (*Lüth*), ECLI:DE:BVerfG:1951:rs19580115.1bvr040051.
[87] Zie ook: BVerfG 24. March 1976, 2 BvR 804/75 (*Zwangsversteigerung I).*
[88] Quint, P. E. (201), A return to Lüth, in: *Roger Williams University Law Review*, Volume 16, Issue 1

In het *Eppler* arrest stelde het BVerfGE vast dat het algemene persoonlijkheidsrecht een abstract, onbenoemd recht is dat naast dan wel boven de 'benoemde' grondrechten zoals het recht op privacy en vrijheid van meningsuiting bestaat:

"Kommt hiernach eine Verletzung von Einzelgrundrechten nicht in Betracht, so bleibt als Prüfungsmaßstab nur das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verfassungsrechtlich gewährleistete allgemeine Persönlichkeitsrecht. Dieses ergänzt als "unbenanntes" Freiheitsrecht die speziellen ("benannten") Freiheitsrechte, die, wie etwa die Gewissensfreiheit oder die Meinungsfreiheit, ebenfalls konstituierende Elemente der Persönlichkeit schützen. Seine Aufgabe ist es, im Sinne des obersten Konstitutionsprinzips der "Würde des Menschen" (Art. 1 Abs. 1 GG) die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen zu gewährleisten, die sich durch die traditionellen konkreten Freiheitsgarantien nicht abschließend erfassen lassen."[89]

Een bijkomend voordeel van deze interpretatie is dat zij technologie onafhankelijk is en daarmee mee kan groeien met de eisen van de tijd. Daar waar de 'catalogus' van klassieke grondrechten geen effectief antwoord heeft op een schending van de menselijke waardigheid kan het algemene persoonlijkheidsrecht deze ruimte invullen.

5.2.1.2 Polen

In Polen wordt de rechtstreekse werking van grondrechten rechtstreeks door de Poolse grondwet afgedwongen. Artikel 30 van de Poolse Grondwet beschermt de onaantastbare menselijke waardigheid. Artikel 31 van de Poolse Grondwet stelt vervolgens dat eenieder de rechten en vrijheden van anderen dient te respecteren. Hiermee is de horizontale werking van grondrechten constitutioneel geborgd.[90] Er staat evenwel geen directe rechtsgang open voor constitutionele schendingen door private partijen. Hiervoor dient de normale civielrechtelijke route te worden bewandeld. Wanneer een burger deze heeft uitgeput en van mening is dat de lagere gerechten onvoldoende rekening hebben gehouden met zijn of haar constitutionele rechten, dan kan een klacht worden ingediend bij het Constitutionele Hof.[91]

Verder worden persoonlijkheidsrechten (of persoonlijke goederen) specifiek in het Poolse burgerlijk recht onderkend en benoemd. Artikel 23 van het Burgerlijk Wetboek geeft een niet limitatieve lijst van immateriële goederen en rechten als gezondheid, vrijheid, eer, godsdienstvrijheid, (goede) naam, huisrecht en intellectueel eigendom.[92]

5.2.1.3 Verenigd Koninkrijk

Het Verenigd Koninkrijk kent geen geschreven grondwet. Wel heeft de *Human Rights Act 1998 (HRA)* een 'constitutionele status'.[93] De HRA heeft tot doel om de in het EVRM vastgelegde rechten te incorporeren in het Engelse rechtssysteem. Paragraaf 3 van de HRA verplicht de gerechten tot verdragsconforme

[89] BVerfGE 54, 148, 1980 (*Eppler*), via: http://www.servat.unibe.ch/dfr/bv054148.html
[90] Młynarska-Sobaczewska, A. *et al.* (eds) (2015), *Horyzontalne oddziaływanie Konstytucji Rzeczypospolitej Polskiej oraz Konwencji o ochronie praw człowieka i podstawowych wolności*, Biuro Trybunału Konstytucyjnego, p. 25
[91] Ibid. p. 30
[92] łubińska-Jentkiewicz,Karpiuk, *Prawo Nowych Technologii - Wybrane Zagadnienia* (Wolters Kluwer) 324.
[93] Human Rights Act 1998, raadpleegbaar via: http://www.legislation.gov.uk/ukpga/1998/42/contents

interpretatie van het Engelse recht en paragraaf 6 dwingt publieke autoriteiten (waartoe ook de gerechten behoren) om verdragsconform te handelen. Hoewel de horizontale werking van de HRA onderwerp van debat was, is door het Engelse Supreme Court in verschillende zaken de horizontale werking van de HRA (en daarmee grondrechten als het recht op privacy) bevestigd. Het startpunt voor deze doctrine wordt gevormd door twee zaken die privacy als onderwerp hadden: *Douglas v Hello*[94] en *Campbell v MGN*.[95]

5.2.1.4 Zweden

In Zweden is er in de nationale rechtsorde relatief weinig aandacht voor de horizontale werking van het recht op privacy. Uit de Zweedse grondwet is af te leiden dat grondrechten hun werking hebben in verticale verhoudingen. Artikel 6 van de Zweedse Grondwet stelt dat burgers beschermd dienen te worden tegen inmenging in hun persoonlijke levenssfeer door de overheid.[96] Hoewel er in Zweden discussies zijn gevoerd over de rol van de staat bij het beschermen van privacy in horizontale verhoudingen zijn er geen indicaties dat de Zweedse wetgever stappen wil nemen op dit gebied. Via onder andere de werking van het EVRM en Europese instrumenten als de AVG is er desalniettemin sprake van horizontale werking van grondrechten (zie paragraaf 5.2.2).

5.2.1.5 Nederland

In Nederland is de menselijke waardigheid niet als zelfstandig grondrecht benoemd. Als zodanig kon de in Duitsland door het BVerfGE gevolgde redeneertrant dat dit grondrecht tegen eenieder geldt niet gevolgd worden. Met andere woorden, er is geen artikel in onze Grondwet die de basis kan vormen voor een algemeen persoonlijkheidsrecht.[97] Desalniettemin heeft via de jurisprudentie van de Hoge Raad het concept van een algemeen persoonlijkheidsrecht zijn intrede gedaan in Nederland. In het Valkenhorst arrest formuleerde de Hoge Raad het aldus:

"3.2. Uitgangspunt voor de beoordeling van het middel is dat het aan grondrechten als het recht op respect voor het privé leven, het recht op vrijheid van gedachte, geweten en godsdienst en het recht op vrijheid van meningsuiting ten grondslag liggende algemene persoonlijkheidsrecht mede omvat het recht om te weten van welke ouders men afstamt."[98]

Daar waar in bijvoorbeeld Duitsland en Polen de Grondwet de expliciete basis vormt voor het algemene persoonlijkheidsrecht, creëerde de Hoge Raad de figuur van een algemeen persoonlijkheidsrecht dus *extra legem, intra ius*.

[94] [2005] EWCA Civ 595; [2005] 3 WLR 881
[95] *Campbell v MGN* [2004] UKHL 22; [2004] 2 AC 457, available; http://www.bailii.org/uk/cases/UKHL/2004/22.html
[96] Artikel via: https://www.riksdagen.se/globalassets/07.-dokument--lagar/the-instrument-of-government-2015.pdf
[97] Zoals beschreven in hoofdstuk 4 kan uit de parlementaire behandeling wel worden afgeleid dat de wetgever ook horizontale privacybescherming voor ogen had.
[98] Hoge Raad, 15 april 1994 (*Valkenhorst 1*), ECLI:NL:HR:1994:ZC1337

5.2.2 Indirecte horizontale werking van grondrechten via het EVRM[99]

Naast nationale ontwikkelingen op het gebied van de horizontale werking van het recht op privacy spelen ook de ontwikkelingen op het niveau van de Raad van Europa een belangrijke rol voor de Nederlandse rechtspraktijk. Het EVRM is ontwikkeld om individuen, groepen individuen, NGOs en private rechtspersonen tegen de staat te beschermen.[100] Zoals in het voorgaande hoofdstuk beschreven, kunnen op grond van artikel 34 EVRM dan ook alleen zaken worden aangespannen bij het EHRM tegen de Hoge Verdragsluitende Partijen (staten).

In de loop der tijd heeft het EHRM wel 'omwegen' gevonden om het EVRM ook haar werking te laten hebben in horizontale verhoudingen. De eerste is via de positieve verdragsverplichtingen, de tweede door nationale rechters verantwoordelijk te houden voor verdragsconforme interpretatie in uitspraken in horizontale verhoudingen.[101]

5.2.2.1 Positieve verdragsverplichtingen

Het EHRM stelt in haar rechtspraak dat staten zich niet alleen moeten onthouden van mensenrechtenschendingen (negatieve verplichting), maar dat zij ook positieve verplichtingen hebben om te garanderen dat burgers zich onderling kunnen beroepen op deze grondrechten.[102] In overweging 42 van het arrest *K.U v. Finland* onderstreept het Hof de positieve verplichting die de staat heeft bij het beschermen van haar burgers:

"The Court reiterates that, although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life."[103]

Door bijvoorbeeld het waarborgen van het recht op privacy te interpreteren als een positieve verplichting, opende het EHRM de deur voor het erkennen van het recht op privacy in horizontale verhoudingen. Op grond van het EVRM kunnen staten daarmee namelijk worden aangesproken wanneer zij onvoldoende maatregelen hebben getroffen om de bescherming van privacy in horizontale verhoudingen te borgen.[104] Via de band van de positieve verplichtingen sorteert artikel 8 EVRM daarmee eveneens effect in horizontale rechtsverhoudingen.[105] Hoewel voor een schending van het EVRM nog steeds de staat wordt aangesproken, sorteert een dergelijk oordeel ook effect jegens de uiteindelijke normadressaten (de private partijen). Bijvoorbeeld doordat strafbaarstellingen worden ingevoerd of uitgebreid, maar ook

[99] Voor een uitgebreide beschrijving van de werking van het Hof en de ontwikkeling van de rechtspraak in relatie tot artikel 8 EVRM zie hoofdstuk 4.
[100] Gerards, J. (2019), *General principles of the European Convention on Human Rights*, p. 136
[101] Gerards, J. (2019), *General principles of the European Convention on Human Rights*, p. 144
[102] van der Jagt, F. (2013), Het recht op bescherming van persoonsgegevens', in: Gerards e.a. (red), *Grondrechten. De nationale, Europese en internationale dimensie*, Nijmegen: Ars Aequi, p. 164. Zie onder andere: EHRM, 28 oktober 1998, app. no. 23452/94 (*Osman v. het Verenigd Koninkrijk*)
[103] EHRM, 2 december 2008, app. no. 2872/02 (*K.U. v. Finland*)
[104] Zie onder andere: EHRM, 4 maart 2004, app. no. 39272/98 (*M.C. v. Bulgarije*), EHRM, 9 oktober 1979, app. no. 289/73 (*Airey v. Ierland*), EHRM, 26 maar t 1985, app. no. 8978/80 (*X & Y v. Nederland*).
[105] Groothuis, M. M. (2019), *Tekst en Commentaar Grondwet* (online versie)

omdat de vereisten die het EHRM stelt aan de omgang met privacy in horizontale ook hun weg vinden in de nationale rechtspraktijk.[106]

5.2.2.2 Verdragsconforme interpretatie

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.[107]

5.3 Privacy en het algemeen persoonlijkheidsrecht nader bekeken

Hoewel een algemeen persoonlijkheidsrecht in Nederland wordt onderkend, is er geen uitgebreide jurisprudentie over dit recht in relatie tot (horizontale) privacyschendingen. Dit in tegenstelling tot Duitsland waar het recht op informationele zelfbeschikking een belangrijke rechtsfiguur vormt. In de Duitse rechtstraditie vloeien uit het algemene persoonlijkheidsrecht een aantal specifieke (sub)rechten voort. Het gaat om:

1) het recht op *informationalle Selbstbestimmung* (informationele zelfbeschikking)
2) het *Selbstdarstellungsrecht* (het recht op 'zelfweergave')
3) en het *Gegendarstellungsrecht* (het 'rectificatie-' of 'tegenwoord' recht)[108]

Deze driedeling uit de Duitse rechtstraditie kunnen wij gebruiken als kader voor een nadere beschouwing op het algemeen persoonlijkheidsrecht.

5.3.1 Informationalle Selbstbestimmung (informationele zelfbeschikking)

In het *Völkszahlung* arrest stelt het BVerfGE dat uit het algemeen persoonlijkheidsrecht het recht op 'informationele zelfbeschikking' voortvloeit:

1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß.[109]

---

[106] Zie bijvoorbeeld EHRM, app. no. 61496/08 (*Barbalescu v. Roemenië*). De eisen die het Hof stelt in dit arrest aan de omgang met de privacy van werknemers worden door nationale rechters en toezichthouders overgenomen.
[107] Zij bijvoorbeeld EHRM, 24 juni 2004, app. no. 59320/00 (*Von Hannover v. Duitsland*)
[108] Nehmelmann, R. (2002), *Algemeen Persoonlijkheidsrecht: een rechtsvergelijkende studie naar het algemeen persoonlijkheidsrecht in Duitsland en Nederland*, Deventer: Wolters Kluwer
[109] BVerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83

Uiteraard is het recht op informationele zelfbeschikking niet absoluut. Zoals het BVerfGE aangeeft kan een inbreuk in het geval van een 'zwaarwegend algemeen belang' toegestaan zijn. Maar dit is wel een significante drempel.

In Nederland kennen we de 'informationele zelfbeschikking' als zelfstandig recht niet. Wel wordt van tijd tot tijd geopperd om dit recht in Nederland te introduceren. De Commissie Grondrechten in het Digitale Tijdperk (Commissie Franken) zag in 2000 geen reden om artikel 10 Grondwet aan te passen en burgers een recht op informationele zelfbeschikking toe te kennen.[110] De argumentatie voor dit standpunt is dat een recht op informationele zelfbeschikking zeer verstrekkend zou zijn, hetgeen onherroepelijk tot uitgebreide clausulering zou leiden om dit recht weer te kunnen balanceren met andere grondrechten. De Commissie was van mening dat een dergelijk "veel geven en veel terugnemen" voorkomen moest worden.[111] De vraag is ook in hoeverre met de introductie van de AVG een recht op informationele zelfbeschikking in Nederland nog zinvol of haalbaar is. Uitgangspunt van de AVG -welke boven Nederlands recht gaat- is de afweging tussen de rechten en vrijheden van de betrokkene enerzijds en de belangen van verwerkingsverantwoordelijken en derden anderzijds.[112] Overweging 4 van de AVG spreekt in dit kader nadrukkelijk over een belangenafweging:

"De verwerking van persoonsgegevens moet ten dienste van de mens staan. Het recht op bescherming van persoonsgegevens heeft geen absolute gelding, maar moet worden beschouwd in relatie tot de functie ervan in de samenleving en moet conform het evenredigheidsbeginsel tegen andere grondrechten worden afgewogen."[113]

Hierbij wordt niet de hoge lat gelegd van een 'zwaarwegend algemeen belang'.

5.3.2 Selbstdarstellungsrecht (het recht op 'zelfweergave')

Het *Selbstdarstellungsrecht,* ofwel het recht op zelfweergave, is door het BVerfGE in het *Lebach I* arrest als volgt omschreven:

"Jedermann darf grundsätzlich selbst und allein bestimmen, ob und wieweit andere sein Lebensbild im ganzen oder bestimmte Vorgänge aus seinem Leben öffentlich darstellen dürfen"[114]

Het is dus aan de persoon zelf om te bepalen welke informatie hij of zij openbaar maakt en daarmee een beeld van zichzelf te schetsen. Dit recht op zelfweergave impliceert tegelijkertijd een verbodsrecht voor anderen om een beeld neer te zetten van de persoon, in het bijzonder wanneer dit niet accuraat is. Het recht op zelfweergave ook niet absoluut, maar het suggereert wel dat terughoudendheid geboden is

[110] Commissie Grondrechten in het Digitale Tijdperk (2000), *Rapport van de Commissie Grondrechten in het Digitale Tijdperk,* (Commissie Franken)
[111] Commissie Grondrechten in het Digitale Tijdperk (Commissie Franken) (2000), p. 125
[112] De verwerkingsverantwoordelijke is degene die doel en middelen voor het verwerken van persoonsgegevens bepaald. Het is daarmee de primaire normadressaat in de AVG.
[113] Overweging 4, Algemene Verordening Gegevensbescherming 2016/679/EU
[114] BVerfGER 35, 202 (*Lebach I*) via: http://www.servat.unibe.ch/dfr/bv035202.html

wanneer men informatie over anderen bekend maakt. Het recht op zelfweergave als exponent van het recht op privacy dient gewogen te worden tegen het belang van het recht op vrijheid van meningsuiting.

Het recht op zelfweergave omvat ook het recht om gevrijwaard te blijven van niet-gedane uitingen. In het *Eppler* arrest stelde het BVerfGE vast dat het toeschrijven van een uiting aan iemand die deze niet gedaan heeft, een aantasting kan zijn van het algemene persoonlijkheidsrecht.[115]

5.3.3 *Gegendarstellungsrecht* (het 'rectificatie-' of 'tegenwoord' recht)

Een derde onderdeel van het persoonlijkheidsrecht vormt het rectificatie of tegenwoordrecht. Dit recht vormt de 'reactieve' variant van het *Selbstdarstellungsrecht*. Is er een uiting gedaan die in strijd is met het *Selbstdarstellungsrecht*, dan kan daar met het behulp van het *Gegendarstellungsrecht* tegen geageerd worden. Wederom dient er een afweging gemaakt te worden tussen het recht op privacy en het recht op vrijheid van meningsuiting.

Het *Gegendarstellungsrecht* wordt in de Nederlandse context op diverse manieren vormgegeven (strafrechtelijk, civielrechtelijk en via het gegevensbeschermingsrecht). Daar waar het gaat om het inroepen van het rectificatierecht is de civielrechtelijke route tot op heden de meest gangbare gebleken.

Een horizontale privacyschending die bestaat uit het openbaar maken van informatie kan een onrechtmatige daad zijn (6:162 BW). Wanneer een uiting onrechtmatig is dan kan op grond van artikel 6:167 BW de rechter rectificatie vorderen:

"Wanneer iemand krachtens deze titel jegens een ander aansprakelijk is ter zake van een onjuiste of door onvolledigheid misleidende publicatie van gegevens van feitelijke aard, kan de rechter hem op vordering van die ander veroordelen tot openbaarmaking van een rectificatie op een door de rechter aan te geven wijze."

Het rectificatierecht heeft weliswaar werking tussen burgers onderling, maar wordt in de praktijk van oudsher ingeroepen tegen uitgevers in het kader van onrechtmatige perspublicaties. Dit omdat het de uitgevers zijn die de uitingen publiceren en ook in staat zijn om een publicatie in te trekken dan wel een rectificatie uit te doen.

Met de komst van internetplatformen (in het bijzonder de sociale media) is het publiceren van content (inclusief onrechtmatige content) echter toegankelijk geworden voor iedereen. Naast het aanspreken van degene die de onrechtmatige uiting doet, wordt nu in steeds meer gevallen het platform aangesproken via welke de onrechtmatige uiting door een derde is gedaan (zie hoofdstuk 10).

Rectificatie kan ook via de band van de AVG afgedwongen worden. De AVG biedt het recht op rectificatie wanneer persoonsgegevens niet accuraat zijn (artikel 16 AVG) en daarenboven het recht op verwijdering (artikel 17 AVG). Artikel 17 lid 2 AVG regelt het 'recht om vergeten te worden' dat specifiek gericht is op het verwijderen van materiaal dat (online) openbaar is gemaakt tegen de wens van de betrokkene in.

[115] BVerfGE 54, 148 (*Eppler*), via: http://www.servat.unibe.ch/dfr/bv054148.html

5.4 Afsluitende beschouwing

Het recht op privacy wordt in alle door ons onderzochte landen grondwettelijk beschermd. De horizontale werking van dit recht wordt in meer of mindere mate ook erkend in alle onderzochte landen. Wel verschilt per land de basis voor deze erkenning. Polen kent de meest directe erkenning van de horizontale werking van het recht op privacy, omdat dit constitutioneel is vastgelegd. In Duitsland vloeit het recht voort uit het recht op de bescherming van de menselijke waardigheid. In Zweden is in de nationale rechtsorde de minste aandacht voor de horizontale werking van grondrechten, maar via het Unierecht en het EVRM wordt ook daar de horizontale werking van grondrechten erkend. In Nederland is de horizontale werking van grondrechten terug te voeren op de door de Hoge Raad erkende notie van het algemeen persoonlijkheidsrecht.

Hoewel de juridische basis voor de horizontale werking van grondrechten per land verschilt, hebben wij niet kunnen vaststellen dat een sterkere (grondwettelijke) verankering van de horizontale werking van grondrechten ook een hoger niveau van bescherming in de praktijk tot gevolg heeft.[116] Dit kan wellicht deels worden verklaard vanuit het feit dat alle onderzochte landen gebonden zijn aan het EVRM. Nu het EHRM expliciet de horizontale werking van grondrechten erkend en alle onderzochte landen gebonden zijn aan het EVRM is er op dit niveau een uniforme basis. Verder is in de onderzochte landen de bescherming van het grondrecht op privacy en gegevensbescherming ook redelijk uniform door de gebondenheid aan het Unierecht.

De grondrechtelijke bescherming van de horizontale privacy krijgt daadwerkelijk gestalte in lagere wetgeving. Hierbij moet primair gedacht worden aan het gegevensbeschermingsrecht, het civiele recht en het strafrecht. In de volgende hoofdstukken gaan wij in op deze verschillende rechtsgebieden en de bescherming die zij burgers bieden tegen privacyschendingen in horizontale verhoudingen.

[116] Hierbij moet wel worden aangetekend dat de bescherming van privacy in de praktijk van tal van factoren afhangt, welke wij niet allemaal in onze analyse hebben kunnen betrekken.

6 Gegevensbeschermingsrecht

Het gegevensbeschermingsrecht ziet op de bescherming van de gegevens van natuurlijke personen (persoonsgegevens). Omdat er bij horizontale privacyschendingen veelal ook sprake is van de verwerking van persoonsgegevens, verdient het gegevensbeschermingsrecht specifiek aandacht.

Het recht op gegevensbescherming wordt met name door de Europese Unie gereguleerd. In het Handvest van de grondrechten van de Europese Unie is het recht op gegevensbescherming expliciet ontkoppeld van het recht op privacy. In artikel 16 van het werkingsverdrag van de Europese Unie staat de bevoegdheid van de EU om het gegevensbeschermingsrecht nader te reguleren. Dat is gedaan door middel van de Algemene verordening gegevensbescherming (AVG).[117] Hieronder wordt nader ingegaan op de achtergrond en het toepassingsbereik van de AVG en de beginselen, de plichten en de rechten die daarin zijn vervat. In tabel 6.1 staan de belangrijkste bepalingen omtrent privacy- en gegevensbescherming binnen de EU.

Artikel 7 Handvest: Eerbiediging van het privéleven en het familie- en gezinsleven [118]	**Artikel 8 Handvest: Bescherming van persoonsgegevens**	**Artikel 16 Werkingsverdrag[119]**
Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.	1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens. 2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan. 3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.	1. Eenieder heeft recht op bescherming van zijn persoonsgegevens. 2. Het Europees Parlement en de Raad stellen volgens de gewone wetgevingsprocedure de voorschriften vast betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de lidstaten, bij de uitoefening van activiteiten die

[117] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119)
[118] Handvest van de grondrechten van de Europese Unie (2012/C 326/02), via: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A12012P%2FTXT
[119] Geconsolideerde versie van het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie, Publicatieblad Nr. C 326 van 26/10/2012 blz. 0001 – 0390, via: https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:12012E/TXT&from=NL

		binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrij verkeer van die gegevens. Op de naleving van deze voorschriften wordt toezicht uitgeoefend door onafhankelijke autoriteiten. De op basis van dit artikel vastgestelde voorschriften doen geen afbreuk aan de in artikel 39 van het Verdrag betreffende de Europese Unie bedoelde specifieke voorschriften.

Tabel 6.1 De belangrijkste bepalingen aangaande privacy-en gegevensbescherming in de EU

6.1 Achtergrond

Hoewel privacy en gegevensbeschermingsrecht nauw met elkaar verbonden zijn, valt het recht op gegevensbescherming niet 'onder' het recht op privacy. Privacy gaat om de integriteit van het lichaam, de bescherming van de woning, het briefgeheim, de persoonlijke levenssfeer en over gegevens die privé of gevoelig zijn. Het recht op gegevensbescherming betreft de bescherming van in beginsel alle informatie over personen, met inbegrip van openbare en niet-gevoelige gegevens, terwijl onder het recht op privacy alleen gegevens over personen worden beschermd als die iemands persoonlijke leven kunnen raken. Een tweet lezende: *"Kijk, Hugo de Jonge heeft groene schoenen aan",* raakt wel aan het recht op gegevensbescherming, maar niet aan het recht op privacy.

De AVG is een 'verordening'. De vorige gegevensbeschermingsregels uit de EU stonden in een 'richtlijn', namelijk de Richtlijn bescherming persoonsgegevens uit 1995.[120] Die richtlijn was in Nederland geïmplementeerd in de Wet bescherming persoonsgegevens. Dat is gelijk het belangrijkste verschil tussen een verordening en een richtlijn. Een verordening werkt in de hele EU en de regels die daarin staan hoeven niet nog eens in een nationale wet te worden aangenomen. Bij een richtlijn moet dat wel. Slechts op een aantal punten, waar de AVG expliciet aangeeft dat landen speciale regels mogen aannemen, mogen er nationale wetten komen. Voorbeelden zijn regels over het verwerken van bijzondere persoonsgegevens (over iemands ras, geaardheid, medische gezondheid, *et cetera*) en regels over hoe de vrijheid van meningsuiting zich verhoudt tot het recht op gegevensbescherming. In Nederland zijn deze nationale regelingen vastgelegd in de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG).

De regels uit de richtlijn en de verordening zijn in wezen hetzelfde, al zijn ze hier en daar wat meer verduidelijkt en aangescherpt. De AVG is van toepassing op natuurlijke en rechtspersonen (burgers,

[120] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens

bedrijven en overheidsorganisaties) die persoonsgegevens verwerken (de zogenaamde verwerkingsverantwoordelijke). De verordening is dus direct relevant voor horizontale verhoudingen.

Het belangrijkste probleem met de regels uit de Richtlijn bescherming persoonsgegevens en de Wet bescherming persoonsgegevens was dat ze simpelweg niet werden nageleefd en beperkt werden gehandhaafd. Omdat verschillende landen verschillende regels hadden, vestigden bedrijven zich vaak in de landen met de laagste wettelijke vereisten.[121] Ook waren er weinig handhavingsmogelijkheden voor de overheid om de regels af te dwingen. De pakkans bij een overtreding van de regels was klein en de boetes die erop volgden bedroegen maximaal een paar duizend euro. Nu is dat veranderd. De Verordening trekt de regels voor de hele EU gelijk, geeft meer mogelijkheden voor handhavingsorganisaties om samen te werken en geeft hun meer middelen en mogelijkheden om op te treden bij een geconstateerde overtreding. Boetes kunnen aanzienlijk zijn, oplopend tot 20 miljoen euro per overtreding, of een percentage van de omzet. Dergelijke boetes hebben een afschrikwerkende werking op verwerkingsverantwoordelijken (met name bedrijven) en dragen daarmee mogelijk bij aan de bescherming van de privacy in horizontale verhoudingen.

6.2 Toepasselijkheid

De AVG is van toepassing als aan vier voorwaarden is voldaan: 1) er is sprake van persoonsgegevens, die 2) verwerkt worden, 3) binnen het territoriale en 4) materiële toepassingsbereik van de Verordening.

6.2.1 Er is sprake van 'persoonsgegevens'

Wil de AVG van toepassing zijn dan moet er allereerst sprake zijn van een 'persoonsgegeven'. Een persoonsgegeven is kort gezegd informatie over een specifiek individu. Het gaat dan om informatie over 'natuurlijke personen' en niet over 'rechtspersonen'.[122] In sommige gevallen kan informatie over een rechtspersoon toch als persoonsgegeven worden gezien, namelijk als de informatie over een rechtspersoon iets zegt over een persoon van vlees en bloed. Het gaat in de AVG ook alleen over informatie over nog levende personen. Informatie over overleden personen valt in principe niet onder de reikwijdte van de Verordening. In sommige gevallen kan informatie over overleden personen toch als een persoonsgegeven worden gezien, namelijk als die informatie iets zegt over een nog levend persoon. "De moeder van Marietje is overleden aan een erfelijke vorm van borstkanker" is zo'n voorbeeld.

Algemene informatie of informatie over objecten valt in principe niet onder het begrip persoonsgegeven. De zin *"Er wonen 18 miljoen mensen in Nederland"* is zo algemeen dat het geen persoonsgegeven is.

[121] Overweging 9 AVG zegt daarover: *"De doelstellingen en beginselen van Richtlijn 95/46/EG blijven overeind, maar de richtlijn heeft niet kunnen voorkomen dat gegevens in de Unie op gefragmenteerde wijze worden beschermd, dat er rechtsonzekerheid heerst of dat in brede lagen van de bevolking het beeld bestaat dat met name online-activiteiten aanzienlijke risico's voor de bescherming van natuurlijke personen inhouden. De lidstaten bieden op het vlak van verwerking van persoonsgegevens uiteenlopende niveaus van bescherming van de rechten en vrijheden van natuurlijke personen, met name de bescherming van persoonsgegevens, wat het vrije verkeer van persoonsgegevens binnen de Unie in de weg kan staan. Die verschillen kunnen dan ook een belemmering vormen voor de uitoefening van economische activiteiten op Unieniveau, de mededinging verstoren en de overheid beletten de taak die zij uit hoofde van het Unierecht heeft, te vervullen. Die verschillende beschermingsniveaus zijn toe te schrijven aan de verschillen in de uitvoering en toepassing van Richtlijn 95/46/EG."*

[122] Zoals het landenrapport voor het Verenigd Koninkrijk aangeeft kan regelgeving omtrent vertrouwelijkheid wel van toepassing zijn op bedrijfsgeheimen en andere informatie over rechtspersonen.

Informatie over een kleine groep mensen kan dat weer wel zijn. Een voorbeeld is: *"In deze straat heeft 90% een crimineel verleden"*. Dan is de groep klein genoeg om met redelijke zekerheid iets te zeggen over een persoon in die straat. Ook is de kans redelijk groot dat de informatie over het crimineel verleden op individuen van toepassing is. Waar de grens precies ligt - hoe klein de groep personen moet zijn en hoe hoog de kans moet zijn dat informatie over die groep op een specifiek individu van toepassing is - hangt af van de context. Als de informatie wordt gebruikt om beslissingen te nemen over een individu of een groep dan zal die doorgaans als persoonsgegevens hebben te gelden. Bijvoorbeeld als een verzekeraar besluit geen verzekeringen af te sluiten met mensen die in deze straat wonen.

Belangrijk is dat het bij een persoonsgegeven ook kan gaan om informatie over een persoon, zonder dat je de naam of identiteit van die persoon weet. Zolang je in staat bent om de persoon uniek van anderen te onderscheiden is er sprake van het verwerken van persoonsgegevens.[123] Ook kan het gaan om hele ongevoelige informatie die openbaar toegankelijk is voor iedereen. Bij het gegevensbeschermingsrecht bestaat geen ondergrens (*ratione persona*), zoals bij privacy het geval is. Elke verwerking van persoonsgegevens valt onder het gegevensbeschermingsrecht, ongeacht of dit schade aan de betrokkene toebrengt.

Daarbij komt dat ook gegevens over 'identificeerbare' personen onder het begrip 'persoonsgegeven' vallen. Dat wil zeggen, informatie over een persoon die op dit moment nog niet geïdentificeerd is, maar je dit wel zonder onevenredige inspanning zou kunnen doen. Als je bijvoorbeeld twee aparte databases hebt die elk afzonderlijk niemand kunnen identificeren, maar als ze worden samengevoegd wel, dan kan het zijn dat die databases moeten worden gezien als bevattende persoonsgegevens, zelfs nog voor het moment dat ze worden samengevoegd. Encryptie (het versleutelen van gegevens) of het pseudonimiseren (in plaats van te spreken over mevrouw De Wit een code als 'SU*###' te gebruiken) van gegevens betekent niet dat zij niet langer als persoonsgegevens zijn aan te merken.

6.2.2 Er is sprake van het 'verwerken' van persoonsgegevens

De AVG alleen van toepassing als die persoonsgegevens ook worden 'verwerkt'. Dat is een zeer breed begrip: bijna alles wat je kunt doen met gegevens valt onder het begrip verwerking. Het gaat dan om het verzamelen van gegevens, het opslaan van gegevens, het samenvoegen van datasets en het doorsturen van de gegevens, maar ook om het verwijderen van de gegevens en het wissen of vernietigen van gegevens. Kortom, vrijwel alles is te zien als een verwerking.

De AVG gaat in ieder geval om alle verwerkingen die geautomatiseerd of gedeeltelijk geautomatiseerd plaatsvinden. Ook is de Verordening op gegevensverwerking op 'papier' van toepassing als de gegevens in een geordende en gestructureerde vorm worden bewaard, zoals een archief (een bestand). Aangezien deze studie met name ziet op privacygevaren door de inzet van digitale apparatuur of diensten zal deze voorwaarde geen belemmering vormen.

[123] Zie: Schermer, B. W., Hagenauw, D., Falot, N. (2018) *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*, Ministerie van Justitie en Veiligheid

6.2.3 De verwerking valt onder het territoriaal toepassingsbereik

De AVG heeft alleen betrekking op de verwerking van persoonsgegevens op EU grondgebied of als de verwerking burgers in de Unie treft. De meest basale regel is dat de AVG van toepassing is op burgers en organisaties die in een van de lidstaten van de EU zijn gevestigd en persoonsgegevens verwerken (ongeacht of zij persoonsgegevens van burgers in de Unie verwerken, of van personen buiten de Unie).[124] Daarvan zal in veruit de meeste van de in deze studie beschreven gevallen sprake van zijn.

Daarnaast zijn er nog twee gevallen voor deze studie relevant waarin de AVG ook van toepassing is.

- Ten eerste is de AVG van toepassing wanneer een organisatie geen vestiging heeft in de EU, maar wel goederen of diensten aanbiedt in de Unie. Bijvoorbeeld, Amazon heeft geen vestiging in de EU, maar runt wel Amazon.de die op een specifiek Duits publiek is gericht en verwerkt in het kader daarvan de gegevens van Duitse klanten.
- Ten tweede is de AVG van toepassing wanneer een organisatie geen vestiging heeft in de EU, maar wel persoonsgegevens over burgers in de Unie verwerkt door het monitoren van hun gedrag. Het gaat dan om gedrag dat in de EU plaatsvindt. Bij het monitoren van gedrag gaat het met name om internet monitoring, bijvoorbeeld het door middel van cookies.

6.2.4 De verwerking valt binnen het materiële toepassingsbereik

De AVG is in beginsel van toepassing op elke verwerking van persoonsgegevens. Wel is er een aantal uitzonderingen op het materiële toepassingsbereik van de AVG. Daarvan is er een voor deze studie met name relevant. Artikel 2 AVG stelt:

"Deze verordening is niet van toepassing op de verwerking van persoonsgegevens (…) door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit."[125]

Daarbij geeft overweging 18 nadere duiding:

"Tot persoonlijke of huishoudelijke activiteiten kunnen behoren het voeren van correspondentie of het houden van adresbestanden, het sociaal netwerken en online-activiteiten in de context van dergelijke activiteiten. Deze verordening geldt wel voor verwerkingsverantwoordelijken of verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten."[126]

Derhalve geldt dat voor zover producten of diensten worden gebruikt op een wijze waarbij persoonsgegevens over derden worden verzameld voor persoonlijke of huishoudelijke doeleinden, de AVG, de UAVG niet van toepassing zijn. Daarbij valt te denken aan een persoonlijk adresboek met daarin

[124] Interessant is dat de verwerkingsverantwoordelijke een natuurlijke of een rechtspersoon kan zijn, maar dat het artikel over het territoriale toepassingsbereik enkel spreekt over 'een vestiging van een verwerkingsverantwoordelijke'. Dit lijkt te impliceren dat de wetgever onbewust primair rechtspersonen op het oog heeft gehad als het gaat om de toepassing van de AVG, daar natuurlijke personen doorgaans geen 'vestiging' hebben.
[125] Artikel 2 AVG.
[126] Overweging 18 AVG.

de adressen van familie of vrienden, of het filmen van het eigen gezin. Toch zijn er in de jurisprudentie de nodige beperkingen op deze uitzonderingsgrond neergelegd. Daarbij zijn met name twee restricities van het Europees Hof van Justitie van belang.

De eerste restrictie volgt uit de zaak Bodil Lindqvist uit 2003.[127] In deze zaak ging het om mevrouw Lindqvist die een openbare website bijhield waarin ze vertelde over haar werk voor de plaatselijke kerkgemeenschap. Ze deelde op deze site ook met naam en toenaam gegevens over haar collega's, onder meer dat één van hen medisch verlof had gekregen voor een voetblessure. De vraag was of een dergelijke handeling onder de huishoudelijke exceptie viel, nu het doeleinde waarvoor de gegevens werden verwerkt primair persoonlijk was: de internetpagina was immers primair voor mevrouw Lindqvist en een kleine kring bekenden bedoeld. Het Hof van Justitie ging daar echter niet in mee en stelde dat:

"*Die uitzondering moet derhalve aldus worden uitgelegd, dat zij uitsluitend betrekking heeft op activiteiten die tot het persoonlijke of gezinsleven van particulieren behoren, hetgeen klaarblijkelijk niet het geval is met de verwerking van persoonsgegevens die bestaat in hun openbaarmaking op internet waardoor die gegevens voor een onbepaald aantal personen toegankelijk worden gemaakt.*"[128]

Het openbaar maken van gegevens aan een onbepaalde groep mensen is in ieder geval géén verwerking voor puur persoonlijke of huishoudelijke doeleinden, al was het maar omdat de verdere verwerking niet kan worden begrensd voor wat betreft die doeleinden.

Ook als persoonlijke informatie wordt gedeeld met mensen buiten een kleine kring van vrienden en familieleden zal de verwerking niet snel onder de huishoudelijke exceptie vallen. Zo gaf de voormalige *Article 29 Working Party*, het adviesorgaan op het gebied van gegevensbescherming in de Europese Unie, bijvoorbeeld ten aanzien van Social Network Sites (SNS) aan dat die sites:

"standaard en gratis privacy-vriendelijke settings dienen te hanteren die de toegang tot informatie limiteren tot de door gebruikers geselecteerde contacten. Wanneer toegang tot profielinformatie verder gaat dan deze contacten, zoals wanneer toegang tot het profiel wordt geboden aan alle deelnemers van een SNS of wanneer de data wordt geïndexeerd door zoekmachines, dan gaat de toegang verder dan de persoonlijke of huishoudelijke sfeer. Als een gebruiker zelf informatie deelt buiten de cirkel van geselecteerde vrienden, dan zal hij als verantwoordelijke worden aangemerkt. Effectief zal dan hetzelfde juridische regime van toepassing zijn als wanneer een person een ander technologisch platform gebruikt om persoonlijke informatie te publiceren op het web."[129]

Een tweede restrictie volgt uit de zaak Ryneš uit 2013.[130] De zaak draaide om een persoon die een camera had gericht op de toegang tot zijn erf, voor beveiligingsdoeleinden. Wederom was de vraag of deze

[127] EHvJ, 6 november 2003, zaaknummer C-101/01, ECLI:EU:C:2003:596 (*Bodil Lindqvist*)
[128] EHvJ, 6 november 2003, zaaknummer C-101/01, ECLI:EU:C:2003:596 (*Bodil Lindqvist*), r.o. 47
[129] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, 01189/09/EN WP 163, 12 June 2009, Brussel. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf>. Citaat vertaald door onderzoekers op verzoek van het WODC.
[130] EHvJ, zaaknummer C-212/13, 11 december 2014, ECLI:EU:C:2014:2428, (*Ryneš*)

toepassing onder de huishoudelijke exceptie viel, nu het doel van de werking van persoonsgegevens (*in casu* van mensen die toegang zochten tot het huis) primair van persoonlijke aard was en de gegevens niet waren bedoeld om openbaar te worden gemaakt. Het Hof oordeelde dat ook hier de huishoudelijke exceptie niet van toepassing was:

"Voor zover het gebruik van een videobewakingssysteem, zoals dat in het hoofdgeding, de openbare ruimte bestrijkt – zelfs gedeeltelijk – en hierdoor buiten de privésfeer geraakt van degene die door middel van dit systeem gegevens verwerkt, kan het niet worden beschouwd als een activiteit die met uitsluitend „persoonlijke of huishoudelijke doeleinden" wordt verricht".[131]

Dat betekent dus in ieder geval dat in zoverre bijvoorbeeld slimme deurbellen deels zijn gericht op de openbare ruimte, de gegevensverzameling die daarmee geschiedt niet onder de huishoudelijke exceptie zal vallen. Datzelfde geldt waarschijnlijk, *mutatis mutandis*, voor gevallen waarin niet de openbare ruimte, maar de privéruimtes van anderen worden gefilmd.

Tot slot is voor privacyschendingen in horizontale verhoudingen nog relevant dat het recht op gegevensbescherming kan botsen met andere grondrechten (dit geldt ook ten aanzien van het recht op privacy, als dat wordt toegepast binnen horizontale verhoudingen). Bij bedrijven valt daarbij te denken aan het recht op ondernemerschap, zoals onder meer is vervat in artikel 16 van het Handvest van de Fundamentele Rechten van de Europese Unie:

> *"De vrijheid van ondernemerschap wordt erkend overeenkomstig het recht van de Unie en de nationale wetgevingen en praktijken."*

In burger-burger relaties zal het daarbij met name gaan om het recht op vrijheid van meningsuiting, zoals onder meer neergelegd in artikel 11 van dat Handvest:

> *"1. Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te hebben en de vrijheid kennis te nemen en te geven van informatie of ideeën, zonder inmenging van enig openbaar gezag en ongeacht grenzen.*
> *2. De vrijheid en de pluriformiteit van de media worden geëerbiedigd."*

Onder het recht op de vrijheid van meningsuiting valt immers ook het recht op het vergaren en het verspreiden van informatie.

De AVG geeft aan dat landen nadere regels kunnen stellen ten aanzien van de verwerking van persoonsgegevens voor dergelijke doeleinden. Opvallend is dat Nederland er in de UAVG voor heeft gekozen om slechts voor journalistieke werkzaamheden uitzonderingen op het gegevensbeschermingsrecht neer te leggen en niet voor activiteiten in het kader van vrijheid van meningsuiting in het algemeen. In tabel 6.2 zijn de relevante bepaling uit de AVG en de UAVG vervat.

[131] EHvJ, zaaknummer C-212/13, 11 december 2014, ECLI:EU:C:2014:2428, (*Ryneš*), R.o. 33

AVG	UAVG
Artikel 85 Verwerking en vrijheid van meningsuiting en van informatie	Artikel 43. Uitzonderingen inzake journalistieke doeleinden of academische, artistieke of literaire uitdrukkingsvormen
1. De lidstaten brengen het recht op bescherming van persoonsgegevens overeenkomstig deze verordening wettelijk in overeenstemming met het recht op vrijheid van meningsuiting en van informatie, daaronder begrepen de verwerking voor journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen. 2. Voor verwerking voor journalistieke doeleinden of ten behoeve van academische, artistieke of literaire uitdrukkingsvormen stellen de lidstaten uitzonderingen of afwijkingen vast van hoofdstuk II (beginselen), hoofdstuk III (rechten van de betrokkene), hoofdstuk IV (de verwerkingsverantwoordelijke en de verwerker), hoofdstuk V (doorgifte van persoonsgegevens naar derde landen of internationale organisaties), hoofdstuk VI (onafhankelijke toezichthoudende autoriteiten), hoofdstuk VII (samenwerking en coherentie) en hoofdstuk IX (specifieke gegevensverwerkingssituaties) indien deze noodzakelijk zijn om het recht op bescherming van persoonsgegevens in overeenstemming te brengen met de vrijheid van meningsuiting en van informatie. 3. Elke lidstaat deelt de Commissie de overeenkomstig lid 2 vastgestelde wetgevingsbepalingen mee, alsook onverwijld alle latere wijzigingen daarvan.	Deze wet, met uitzondering van de artikelen 1 tot en met 4 en 5, eerste en tweede lid, is niet van toepassing op de verwerking van persoonsgegevens voor uitsluitend journalistieke doeleinden en ten behoeve van uitsluitend academische, artistieke of literaire uitdrukkingsvormen. 2De navolgende hoofdstukken en artikelen van de verordening zijn niet van toepassing op de verwerking van persoonsgegevens voor uitsluitend journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen: a.artikel 7, derde lid, en artikel 11, tweede lid: b.hoofdstuk III; c.hoofdstuk IV, met uitzondering van de artikelen 24, 25, 28, 29 en 32; d.hoofdstuk V; e.hoofdstuk VI; en f.hoofdstuk VII. 3De artikelen 9 en 10 van de verordening zijn niet van toepassing voor zover de verwerking van de in die artikelen bedoelde gegevens noodzakelijk is voor het journalistieke doel of de academische, artistieke of literaire uitdrukkingsvorm.

Tabel 6.2 Beperkingen in het kader van de vrijheid van meningsuiting

In hoeverre er dus sprake kan zijn van een uitzondering voor het verwerken van persoonsgegevens door burgers voor niet journalistieke werkzaamheden die desalniettemin zijn te kwalificeren als de verwerking van persoonsgegevens in het kader van de vrijheid van meningsuiting, blijft onduidelijk. Wel is duidelijk dat burgers zich in een conflict waarbij de ene burger ongewenst persoonsgegevens verzamelt van de

andere burger, zich zullen beroepen op het grondwettelijke recht op gegevensbescherming enerzijds en het grondwettelijke recht op vrijheid van meningsuiting anderzijds. Daarbij verwijzend naar ofwel de Nederlandse Grondwet, ofwel het Handvest van de grondrechten van de Europese Unie, ofwel het Europees Verdrag voor de Rechten van de Mens. Via die lijn zou dan eventueel alsnog een beperking ten aanzien van de gegevensbeschermingsregels kunnen worden afgedwongen.

Voor journalisten geldt dat zij, voorover zij persoonsgegevens verwerken voor journalistieke doeleinden, ontheven kunnen zijn van een groot aantal van de verplichtingen die de AVG aan hen oplegt. Toch benadrukt de Leidraad van de Raad voor de Journalistiek expliciet dat journalisten te alle tijden zijn gehouden aan het respect voor privacy:

"In een publicatie mag de privacy van personen niet verder worden aangetast dan in het kader van de berichtgeving redelijkerwijs noodzakelijk is. Een inbreuk op de privacy is onzorgvuldig wanneer deze niet in redelijke verhouding staat tot het maatschappelijk belang van de publicatie. Journalisten publiceren geen foto's en zenden geen beelden uit die zijn gemaakt van personen in niet algemeen toegankelijke ruimten zonder hun toestemming, en gebruiken evenmin brieven en persoonlijke aantekeningen zonder toestemming van betrokkenen. Journalisten mogen personen niet langdurig lastig vallen, hinderlijk volgen of schaduwen. Journalisten dienen te voorkomen dat informatie of beelden worden gepubliceerd waardoor verdachten en veroordeelden door het grote publiek eenvoudig kunnen worden geïdentificeerd en getraceerd."[132]

Ook journalisten zijn dus, voor zover dat hun werkzaamheden niet ondermijnt, gehouden aan privacy- en gegevensbeschermingsprincipes.

6.2.5 Verwerkingsverantwoordelijke

Als er persoonsgegevens worden verwerkt, de AVG territoriaal van toepassing is en de huishoudelijke of journalistieke exceptie niet van toepassing zijn, dan moet de AVG worden gerespecteerd. Dat dient in ieder geval te gebeuren door de zogenoemde 'verwerkingsverantwoordelijke'. Er is altijd een verwerkingsverantwoordelijke voor de gegevensverwerking, de vraag is alleen wie dat is. Vaak is dat simpel, bijvoorbeeld als er maar één burger of organisatie bij de verwerking van persoonsgegevens betrokken is. Soms is het ingewikkelder en zijn er meerdere organisaties in het spel. Dan zijn er twee opties:

1. ofwel ze zijn allemaal aan te merken als individuele verwerkingsverantwoordelijke, dan wel als gezamenlijke verwerkingsverantwoordelijken (artikel 24 AVG);
2. ofwel één of meer partijen zijn niet als verwerkingsverantwoordelijke aan te merken maar als 'verwerker' (artikel 28).[133]

Een 'verwerker' is kort gezegd een persoon of organisatie die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Als Philips het bedrijf Data Storage BV vraagt om gegevens van Philips in een datacentrum op te slaan, dan is Data Storage BV de verwerker en Philips

[132] Leidraad van de Raad voor de Journalistiek December 2019. Bij deze bepalingen wordt we aangegeven dat: *Het afwijken van deze norm kan worden gerechtvaardigd wanneer er evident sprake is van een misstand én wanneer dit noodzakelijk is om de desbetreffende kwestie aan de orde te stellen.*
[133] Zie ook: 82 lid 4 AVG

de verwerkingsverantwoordelijke. De verwerker mag alleen in opdracht van de verantwoordelijke handelen en voert dus slechts de contractuele afspraken uit.

De verwerker heeft een aantal plichten onder de AVG, zoals het goed beveiligen van de gegevens, het melden van fouten en misstanden, het respecteren van de rechten van personen over wie gegevens worden verwerkt en (afhankelijk van de omstandigheden) het aanstellen van een functionaris voor de gegevensbescherming.

De verwerkingsverantwoordelijke, de naam zegt het al, is verantwoordelijk voor het gegevensverwerkingsproces. Als de verwerker een fout maakt dan wordt de verwerkingsverantwoordelijke daar in eerste instantie op aangesproken. Verwerkingsverantwoordelijke is degene die besluit tot het verwerken van de persoonsgegeven, bijvoorbeeld Philips dat besluit klantgegevens te verzamelen door middel van een klanttevredenheidsonderzoek. Het gaat dus om de organisatie die het doel en de middelen van de verwerking vaststelt, dat wil zeggen waarom de gegevens worden verwerkt en hoe.

Als er meerdere organisaties als vererkingsverantwoordelijke zijn aan te merken, bijvoorbeeld als Philips en de gemeente Eindhoven samen besluiten om te bestuderen hoe burgers van de gemeente Eindhoven reageren op veranderingen in de kleur van de straatverlichting, dan moeten de verschillende rollen contractueel worden vastgelegd. Zodoende is achteraf duidelijk wie waarvoor aansprakelijk kan worden gehouden.

Bij de meeste privacyschendingen in horizontale verhoudingen zal het eenvoudig zijn: de burger die gegevens verwerkt is de verwerkingsverantwoordelijke en er zijn weinig andere partijen bij betrokken. Als informatie wordt gedeeld op sociale media kan dat echter anders liggen. Zo stelde de voormalige Artikel 29 Werkgroep dat Social Network Sites (SNS) doorgaans ook als verwerkingsverantwoordelijke moeten worden gezien:

"They provide the means for the processing of user data and provide all the "basic" services related to user management (e.g. registration and deletion of accounts). SNS providers also determine the use that may be made of user data for advertising and marketing purposes - including advertising provided by third parties.[134]

Eenzelfde redenering geldt voor *Internet of Things* toepassingen waarbij de burger het slimme apparaat gebruikt, maar de leverancier allerhande persoonsgegevens verwerkt om het apparaat goed te laten werken. Een goed voorbeeld hiervan zijn digitale assistenten zoals Amazon Alexa: deze apparaten verwerken de vragen van gebruikers om antwoorden te kunnen geven. Zowel de gebruiker als Amazon zijn als verwerkingsverantwoordelijke aan te wijzen als de AVG van toepassing is.

6.3 Beginselen

De AVG kent een aantal belangrijke uitgangspunten waarop de hele Verordening is gebaseerd, te weten:

- Rechtmatigheid: de gegevensverwerking moet rechtmatig zijn. Dat betekent dat er een legitiem doel moet zijn voor de verwerking van (bijzondere) persoonsgegevens en dat alle andere in Europa en Nederland geldende wetten worden nageleefd.

[134] Groep gegevensbescherming Artikel 29, *Opinion 5/2009 on social networking*, 01189/09/EN WP 163

- Behoorlijkheid: oneerlijke handelspraktijken waarbij de consument wordt misleid of waarin een marktpartij misbruik maakt van zijn machtspositie zijn verboden, wat ook geldt voor het opstellen van oneerlijke algemene voorwaarden, waarbij de consument bijvoorbeeld in de *terms and conditions* van een zaklamp-app toestemming wordt gevraagd om meer dan honderd partijen toegang te geven tot alle op zijn telefoon opgeslagen informatie. Dat heeft niks met de zaklampapp te maken en is dus onbehoorlijk (en niet noodzakelijk).
- Doelspecificatie: de gegevensverwerking moet een specifiek doel dienen. Dat doel moet van tevoren worden vastgesteld en specifiek zijn. Niet specifiek genoeg zijn algemene doelen zoals 'klantencontact', 'productverbetering', 'innovatie' of 'reclamedoeleinden'. Een concreet doel kan zijn: "Wij hebben uw adres nodig om het door u bestelde boek te kunnen leveren".
- Doelbinding: de gegevens mogen vervolgens in principe alleen voor het vastgelegde doel worden verwerkt. De adresgegevens om het boek te leveren mogen niet worden doorverkocht aan een bedrijf dat de gegevens gebruikt voor advertentiedoeleinden.
- Dataminimalisatie: het uitgangspunt is dat alleen die gegevens mogen worden verwerkt die noodzakelijk/toereikend zijn om het doel te bereiken.
- Correct en actueel: de gegevens die worden verzameld, moeten correct zijn. Als de verwerkingsverantwoordelijke informatie over een persoon verwerkt moet deze er voor zorgen dat die informatie klopt. Als de persoonsgegevens voor een langere tijd worden bewaard, dan heeft de verwerkingsverantwoordelijke de plicht om ervoor te zorgen dat de gegevens actueel blijven.
- Opslagbeperking: als de persoonsgegevens niet langer nodig zijn voor het bereiken van het doel waarvoor ze zijn verzameld, dan moeten de gegevens weer worden verwijderd.
- Technologische veiligheid: als de gegevens worden opgeslagen, bijvoorbeeld in een database, register of bestand, dan zullen er technische veiligheidsmaatregelen moeten worden getroffen. Denk daarbij aan encryptie en beveiliging tegen hacks.
- Organisatorische veiligheid: als de gegevens worden opgeslagen, bijvoorbeeld in een database, register of bestand, dan zullen er organisatorische veiligheidsmaatregelen moeten worden getroffen. Denk daarbij aan een *clean desk policy*, wachtwoorden en het loggen van personen die toegang willen tot bestanden en databases.
- Transparantie: de gegevensverwerkingsprocessen moeten transparant zijn.

De AVG werkt deze beginselen verder uit. Vijf zaken zijn daarbij in het bijzonder van belang: 1) er moet sprake zijn van een legitieme grondslag voor de verwerking, 2) de verwerking van bijzondere persoonsgegevens is niet toegestaan zonder uitzonderingsgrond, de 3) gegevens mogen niet buiten de Europese Unie worden gebracht, 4) de verwerkingsverantwoordelijke moet zich houden aan alle verplichtingen uit de AVG en 5) de rechten van betrokkenen moeten worden gerespecteerd.

6.3.1 Legitieme grondslag

Allereerst stelt de AVG dat de verwerking van persoonsgegevens dient te berusten op één van de zes legitieme verwerkingsgrondslagen die in de AVG staan genoemd. Daarvan zijn er in horizontale relaties drie met name relevant: 1) toestemming , 2) uitvoering van de overeenkomst en 3) het gerechtvaardigd belang van de verwerkingsverantwoordelijke.

Ad 1) Toestemming

Ten eerste kan het verwerken van persoonsgegevens legitiem zijn als de betrokkenen hun toestemming hebben gegeven. De vereisten voor een rechtsgeldigde toestemming zijn:[135]

- Vrij: Ten eerste moet de toestemming 'vrij' zijn gegeven door een betrokkene. Toestemming mag niet onder dreiging tot stand komen of een voorwaarde zijn voor het gebruik maken van diensten waar de burger recht op heeft.
- Specifiek: Daarnaast moet de toestemming 'specifiek' zijn. Bij het geven van toestemming moet het gaan om een specifiek en afgebakend doel waarvoor een specifieke en afgebakende hoeveelheid persoonsgegevens worden verwerkt. Bijvoorbeeld: *"Ik ga akkoord met het maken van een foto tijdens het familiefeest op het moment dat de taart wordt aangesneden"*.
- Geïnformeerd: De toestemming moet 'geïnformeerd' zijn. De betrokkene moet geïnformeerd worden over de gegevens die worden verwerkt en voor welke doeleinden dat gebeurt.
- Ondubbelzinnig: De toestemming moet 'ondubbelzinnig' zijn. Dat betekent dat de toestemming voor het verwerken van persoonsgegevens duidelijk onderscheiden moet zijn van eventuele andere zaken waarvoor toestemming wordt gevraagd en dat de toestemming actief wordt gegeven. *"Stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit mag derhalve niet als toestemming gelden."*[136] Het is dus niet zo dat als mensen tijdens een familiefeest zien dat er een film wordt gemaakt en zij daar niet actief bezwaar tegen maken, dit als impliciete toestemming mag worden gezien.
- Bewijsbaar: De toestemming moet bewijsbaar zijn. Het is aan de om aan te tonen dat de betrokkene inderdaad zijn toestemming heeft gegeven en dat dit legitiem is gebeurd. Als er dus een juridisch conflict is, dan is er een omkering van de bewijslast. Niet de betrokkene moet aantonen dat hij geen (legitieme) toestemming heeft gegeven, maar het is aan de verwerkingsverantwoordelijke om aan te tonen dat dit wel is gebeurd. Dit kan extra documentatie vergen.

Ad 2) Uitvoering van de overeenkomst

Ten tweede kan een verwerking van persoonsgegevens legitiem zijn als de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen. Deze verwerkingsgrondslag is direct gelieerd aan en eigenlijk ook gebaseerd op de toestemming van de betrokkene, maar hiervoor gelden de vereisten aan contractuele toestemming die volgen uit het Burgerlijk Wetboek. Deze komen evenwel in grote lijnen overeen met de hierboven besproken vereisten. Bij deze verwerkingsgrond kan het bijvoorbeeld gaan om een overeenkomst voor het leveren van een GPS-apparaat in de auto waarvoor het nodig is om de locatiegegevens van de auto te verwerken, of om het verwerken van gegevens over een persoon en zijn woning, bijvoorbeeld om een offerte te maken voor het bouwen van een serre.

Ad 3) gerechtvaardigd belang

Ten derde kan het gaan om het geval waarin *"de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de*

[135] Zie artikel 7 AVG.
[136] Overweging 32 AVG.

belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is."[137] In de eerder besproken zaak, waarin het Hof van Justitie bepaalde dat filmen van ruimtes, gedeeltelijke zijnde de openbare ruimte, niet onder de huishoudelijke exceptie valt, merkte het Hof terzijde op dat het in dergelijke gevallen mogelijk is *"rekening te houden met de gerechtvaardigde belangen van de verantwoordelijke voor de verwerking, die, zoals in het hoofdgeding, met name de bescherming van de eigendom, de gezondheid en het leven van de verantwoordelijke en zijn familie betreffen."*[138] Het is echter de vraag of dat ook geldt voor het recreatief gebruik van producten en diensten; zeker als het gaat om het inzetten van producten en diensten in horizontale relaties om anderen doelbewust schade te berokkenen.

6.3.2 Bijzondere persoonsgegevens

Naast 'gewone' persoonsgegevens maakt de AVG nog gewag van 'persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.'[139]

De verwerking van bijzondere persoonsgegevens is in principe verboden. In burger-burger relaties geldt als belangrijkste uitzondering de toestemming van de betrokkene. Hierbij moet zijn voldaan aan de voorgenoemde vereisten van toestemming; de AVG stelt dat het bij bijzondere persoonsgegevens moet gaan om 'uitdrukkelijke toestemming'. Hoewel de AVG geen definitie geeft van uitdrukkelijke toestemming, mogen we aannemen dat hiermee tot uitdrukking wordt gebracht dat de verkregen toestemming nog nadrukkelijker en explicieter moet zijn gegeven dan normaal al het geval is.

Belangrijk voor de kwalificatie als bijzonder persoonsgegeven is dat de AVG in de Overwegingen een belangrijke begrenzing heeft neergelegd:

"*De verwerking van foto's mag niet systematisch worden beschouwd als verwerking van bijzondere categorieën van persoonsgegevens, aangezien foto's alleen onder de definitie van biometrische gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken.*"[140]

6.3.3 Gegevensdoorgifte

De AVG stelt ook dat persoonsgegevens in principe niet naar landen buiten de EU mogen worden doorgevoerd, omdat de Europese Unie met de AVG het hoogste beschermingsniveau van de hele wereld heeft neergelegd. Als de gegevens naar het buitenland worden doorgevoerd, dan worden ze niet of veel minder goed beschermd dan binnen de EU is de angst. Ook hiervoor gelden uitzonderingen. Zo kan de Europese Commissie, een land met een voldoende sterke (gegevensbeschermings)wetgeving 'adequaat'

[137] Artikel 6 lid 1 sub f AVG.
[138] EHvJ, zaaknummer C-212/13, 11 december 2014, ECLI:EU:C:2014:2428, (*Ryneš)*
[139] Artikel 9 lid 1 AVG.
[140] Overweging 51 AVG.

verklaren. Ook kan een specifieke organisatie binnen een niet-adequaat land zich contractueel vastleggen om AVG-achtige regels te hanteren voor het verwerken van persoonsgegevens; gegevens mogen dan naar die organisatie buiten de EU worden doorgevoerd.

6.3.4 Plichten

Er is een aantal specifieke plichten die de verwerkingsverantwoordelijke in acht moet nemen. Het gaat om verantwoordingsplichten, informatieplichten en beveiligingsplichten.

Verantwoordingsplichten

De AVG kent diverse verantwoordingsplichten. Verwerkingsverantwoordelijken moeten bijvoorbeeld een gegevensbeschermingsbeleid opstellen als de aard van de verwerkingen daartoe noopt, een register van de verwerkte gegevens bijhouden en voor hoog risico verwerkingen gegevensbeschermingseffectbeoordelingen uitvoeren (*data protection impact assessments*, of DPIAs).

Informatieplichten

Op het moment dat er gegevens worden verzameld over een individu moet de verwerkingsverantwoordelijke aan het individu duidelijk maken dat er gegevens over hem worden verwerkt, waarom, door wie, aan wie de gegevens worden doorgegeven, op welke verwerkingsgrondslag er een beroep wordt gedaan, hoe lang de gegevens worden bewaard, welke technische en organisatorische veiligheidsmaatregelen er zijn getroffen, *et cetera*. Als de gegevens niet direct van de betrokkene zelf worden verzameld, maar bijvoorbeeld door een database van een andere partij over te nemen of op te kopen, dan moet deze informatie binnen een maand worden medegedeeld, tenzij het voor de verantwoordelijke vrijwel onmogelijk is om te achterhalen over wie de gegevens gaan en hoe die personen kunnen worden bereikt. Als burgers zelf gegevens verzamelen over anderen dan zal van het eerste geval sprake zijn; het heimelijk verzamelen van gegevens over andere burgers is dus nimmer toegestaan (mits de huishoudelijke exceptie niet van toepassing is).

Beveiligingsplichten

Daarnaast dient de verwerkingsverantwoordelijke ook technische en organisatorische veiligheidsmaatregelen (artikel 32 AVG) te treffen die in verhouding staan tot de hoeveelheid en de aard van de gegevens die zij verwerken (des te meer gegevens en des te gevoeliger de verwerkte gegevens, des te sterker deze maatregelen moeten zijn). Wanneer de integriteit, beschikbaarheid of vertrouwelijkheid van gegevens niet meer gegarandeerd kan worden (bijvoorbeeld omdat er sprake is van een hack, of omdat er een laptop is verloren in de trein), dan is er sprake van een inbreuk in verband met persoonsgegevens (een 'datalek'). In de meeste gevallen moet een dergelijk lek worden gemeld bij de Autoriteit persoonsgegevens (artikel 33 AVG) en als er een groot risico is voor de rechten en vrijheden van betrokkenen, ook bij de betrokkenen zelf (artikel 34 AVG).

6.3.5 Rechten

De betrokkene heeft op grond van de AVG een aantal specifieke rechten. Met het oog op de bescherming van de privacy in horizontale verhoudingen zijn deze in het bijzonder relevant.

Voorbeelden zijn het recht op inzage van de gegevens, het recht op een kopie van de gegevens en het recht op informatie over de gegevensverwerking (artikel 15 AVG). Globaal kan de betrokkene vragen om de volgende informatie:

- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens;
- de ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- de bewaartermijn;
- hoe de verwerkingsverantwoordelijke aan de gegevens is gekomen;
- als er computergestuurde besluiten worden genomen, de logica achter die besluiten, en
- als de gegevens worden doorgevoerd naar buiten de EU, welke waarborgen daarvoor gelden.

Daarnaast is er het recht om persoonsgegevens te rectificeren en aan te vullen als ze incorrect of onvolledig zijn (artikel 16 AVG), mag de betrokkene vragen onrechtmatige verwerkingen stop te zetten (artikel 17 AVG), heeft hij/zij het recht om bezwaar aan te tekenen tegen verwerkingen die zijn gebaseerd op de verwerkingsgrond 'gerechtvaardigd belang' (artikel 21 AVG).

Daarnaast is er een aantal rechten dat primair geldt in de relatie betrokkene en bedrijf, zoals het recht op dataportabiliteit (artikel 20 AVG). Als de grondslag op basis waarvan gewone persoonsgegevens of bijzondere persoonsgegevens worden verwerkt de toestemming van de betrokkene of een contractuele relatie is, dan is het uitgangspunt dat de betrokkene zelf de controle houdt over de data die hij heeft verstrekt. Dit recht heeft alleen betrekking op geautomatiseerde verwerking. Als de betrokkene de data zelf heeft gegeven om een bepaalde dienst geleverd te krijgen en dan mag hij ook weer de gegevens terugvragen en meenemen. Als iemand bijvoorbeeld gegevens met Facebook deelt, dan mag hij Facebook vragen om alle gegevens weer terug te geven of door te sturen naar een concurrent, als de betrokkene besluit om op een ander sociaal medium te gaan.

Ook het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming (artikel 22 AVG) geldt in horizontale verhoudingen, maar speelt met name een rol in diagonale verhoudingen, dat wil zeggen tussen burger en bedrijf. Veel besluiten worden tegenwoordig genomen op basis van profielen en computergestuurde processen. Dat mag, maar de AVG vereist wel dat er altijd een mens moet zijn die controleert of het algemene profiel ook op het specifieke individu van toepassing is. Het kan bijvoorbeeld best zijn dat mannen van tussen de 20 en de 30 vaker auto-ongelukken veroorzaken, maar een verzekeraar mag niet automatisch alle verzekeringsaanvragen van mannen tussen de 20 en de 30 weigeren. Er moet altijd worden gecontroleerd of de algemene aanname ook van toepassing is op de specifieke aanvrager. Dit recht (of eigenlijk plicht van de verwerkingsverantwoordelijke) is alleen van toepassing als het gaat om besluiten die rechtsgevolgen hebben of de betrokkene in aanzienlijke mate treffen. Bij 'onbelangrijke' besluiten - zoals het aanbieden van advertenties op basis van profielen - geldt deze plicht doorgaans niet. Ook mag geautomatiseerde besluitvorming bij belangrijke besluiten als dit berust op een expliciete wettelijke bepaling of als de betrokkene daar zelf om heeft gevraagd of mee akkoord is gegaan. Voor geautomatiseerde besluitvorming op basis van bijzondere persoonsgegevens gelden extra strenge voorwaarden.

De AVG kent ook een klachtrecht en een recht op schadevergoeding (artikel 77-82 AVG). De betrokkene heeft allereerst het recht om een klacht in te dienen over een verwerkingsverantwoordelijke bij de Autoriteit persoonsgegevens (AP). De betrokkene kan ook de verwerkingsverantwoordelijke aansprakelijk stellen voor schade bij de rechter. Als de AP een beslissing neemt die de betrokkene onwelgevallig is – de betrokkene meent bijvoorbeeld dat het gerechtvaardigd belang van de verwerkingsverantwoordelijke niet boven zijn eigen belang uitgaat en doet een beroep op zijn recht op bezwaar, maar de AP beslist in zijn nadeel - dan kan de betrokkene dat besluit aanvechten bij de rechter. Dat geldt overigens ook voor de verwerkingsverantwoordelijke. De betrokkene mag in bijzondere gevallen worden vertegenwoordigd in de uitoefening van zijn rechten. Een betrokkene die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op zijn recht op gegevensbescherming heeft het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade. De AVG biedt landen ook de mogelijkheid om regelingen neer te leggen waardoor betrokkenen vertegenwoordigd kunnen worden in hun belangen door bijvoorbeeld burgerrechtenorganisaties. Daar bestaat in een aantal landen al ruime ervaring mee. Zo zijn er in het Verenigd Koninkrijk diverse mogelijkheden voor *class actions* en *opt-out* rechtszaken.[141]

Belangrijk is ook de verdeling van schade onder samenwerkende verwerkingsverantwoordelijken en verwerkers. Artikel 82 AVG bepaalt dat zowel materiële als immateriële schade kan worden geëist als die is geleden als gevolg van onrechtmatige gegevensverwerking. Daarbij is elke verwerkingsverantwoordelijke die bij verwerking is betrokken aansprakelijk voor de schade, terwijl een verwerker slechts aansprakelijk is als die zich ofwel niet heeft gehouden aan de AVG ofwel zich niet heeft gehouden aan de contractuele afspraken met de verwerkingsverantwoordelijke. Bij de aansprakelijkheid geldt een omkering van de bewijslast. Vermoed wordt dat de schade als gevolg van een verwerking de verwerkingsverantwoordelijke of verwerker kan worden toegedicht, tenzij deze kan aantonen op geen enkele wijze verantwoordelijk te zijn voor het schadeveroorzakende feit. Belangrijk is ook dat wanneer meerdere verwerkingsverantwoordelijken of verwerkers bij dezelfde verwerking betrokken zijn en verantwoordelijk zijn voor schade die door verwerking is veroorzaakt, elke verwerkingsverantwoordelijke of verwerker voor de gehele schade aansprakelijk kan worden gehouden. Dat betekent dat de getroffene de gehele schade kan verhalen op één van de partijen, wat zowel in proceskosten en –tijd kan schelen alsook het voordeel biedt dat de meest bemiddelde partij kan worden aangesproken. Het is dan aan die partij om op de andere verwerkingsverantwoordelijken of verwerkers die bij de verwerking waren betrokken het deel van de schadevergoeding verhalen dat overeenkomt met hun deel van de aansprakelijkheid voor de schade.

6.4 Rechtsvergelijking

Omdat de AVG Europees geharmoniseerd is, zijn er geen grote verschillen in het gegevensbeschermingsrecht tussen de verschillende landen uit de rechtsvergelijking.

[141] *Hicham v Elaph Publishing* [2017] EWCA Civ 29 *Lloyd v Google* [2019] EWCA Civ 1599 *One-Step v Morris-Garner [2018] UKSC 20,* via: https://www.supremecourt.uk/cases/uksc-2016-0086.html

Uit ons onderzoek blijkt dat het Verenigd Koninkrijk in zijn wetgeving bredere bescherming biedt aan kinderen, onder meer ten aanzien van internetplatformen.[142] Het Verenigd Koninkrijk heeft ook (strafrechtelijke) consequenties verbonden aan *blagging* (het verkrijgen van persoonlijke informatie door misleiding). *Blagging* kan worden gekwalificeerd als een vorm van oplichting (*fraud*), maar ook als een criminele inbreuk op de gegevensbeschermingswetgeving (zie artikel 170 *Data Protection Act 2018*).[143] De Engelse toezichthouder ICO is daarmee bevoegd en kan boetes uitdelen voor deze onrechtmatige verwerking van persoonsgegevens.[144] Datzelfde geldt voor de her-identificatie (artikel 171 DPA 2018) van geanonimiseerde gegevens en het aanpassen of vernietigen van gegevens om verzoeken van betrokkenen te ontlopen (artikel 172 DPA 2018). Italië kent ook criminele sancties voor overtreding van de gegevensbeschermingswetgeving, bijvoorbeeld voor het op grote schaal illegaal verzamelen van persoonsgegevens.[145] In de Poolse gegevensbeschermingswetgeving is ook een regeling neergelegd omtrent het monitoren van werknemers door werkgevers. Dat mag niet op bepaalde intieme plaatsen (zoals het toilet) en is slechts toegestaan voor een beperkt aantal doeleinden, zoals het beschermen van eigendommen.[146] In Duitsland zijn er aan de ene kant ruime interpretaties voorzien van de mogelijkheden om bijzondere persoonsgegevens te verwerken, aan de andere kant moeten organisaties eerder dan de AVG voorschrijft een Data Protection Officer aanstellen. Ook zijn er extra regels voor video surveillance in de publieke ruimte. Dit mag in principe slechts geschieden door overheidsorganen in het kader van de uitoefening van een publieke taak - denk daarbij primair aan het handhaven van de openbare orde en het voorkomen van criminaliteit - of ten behoeve van het identificeren en toegang verschaffen van personen aan faciliteiten of gebouwen.[147] In Zweden is van oudsher nadruk op openheid en transparantie, wat zich onder meer ook vertaalt naar extra regels omtrent algoritmische transparantie. In Italië, tot slot, blijkt dat er op een aantal punten verdere uitwerking van de gegevensbeschermingsnormen heeft plaatsgehad in de jurisprudentie. Een voorbeeld daarvan is het plaatsen van foto's van kinderen op sociale media door een van de ouders van een van elkaar gescheiden echtpaar, waarbij de andere ouder geen toestemming had gegeven. De rechter benadrukte in de desbetreffende uitspraak niet alleen dat het ontbreken van toestemming van beide ouders een probleem was, maar ook dat de toegang tot de sociale media niet was afgeschermd. Hierdoor had een onbeperkt aantal personen toegang tot het beeldmateriaal en viel misbruik niet uit te sluiten. De rechter leek daarbij zelfs te verwijzen naar de mogelijkheid dat de foto's zouden worden gebruikt en verspreid in pedofielennetwerken.[148] Dit risico zou dus moeten worden meegenomen in het besluit van ouders om foto's van hun kinderen online te plaatsen of te delen met derden.[149]

[142] https://hansard.parliament.uk/lords/2017-12-11/debates/154E7186-2803-46F1-BE15-36387D09B1C3/DataProtectionBill(HL)
[143] http://www.legislation.gov.uk/ukpga/2018/12/section/170/enacted
[144] Zie voor het toepassen van deze bepaling: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/06/former-claims-company-manager-fined-2-000-over-blagging-calls-to-obtain-personal-data/
[145] Zie de artikelen 167-167ter *Codice in materia die protezione dei data personali*
[146] Artikel 22 van de Arbeidswetgeving (*Kodeks pracy*)
[147] Starnecker, 'BDSG § 4 Videoüberwachung Öffentlich Zugänglicher Räume' in: Gola and Heckmann (eds), *Bundesdatenschutzgesetz* (13th edn, 2019) 1
[148] Tribunale di Ravenna, Sentenza 1038 del 15 ottobre 2019; Tribunale di Rieti, sez. Civile, sentenza 6 del 7 marzo 2019
[149] Voor een vergelijkbare zaak in Nederland zie: ECLI:NL:RBGEL:2020:2521

6.5 Afsluitende beschouwing

Zowel het recht op privacy als het recht op gegevensbescherming hebben een zeer brede reikwijdte. Bij het gegevensbeschermingsrecht is van belang dat dit niet van toepassing is als burgers persoonsgegevens over anderen verwerken voor puur persoonlijke doeleinden. Het bijhouden van een adressenlijst van vrienden en kennissen op de computer is daar het voorbeeld *par excellence* van. Bij zowel het privacyrecht als het gegevensbeschermingsrecht geldt dat ze in horizontale relaties kunnen botsen met andere grondrechten. 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.

Voor het recht op privacy is van belang dat het recht beperkt is in de zin dat, uitzonderingen daargelaten, alleen natuurlijke personen voor hun individuele belangen kunnen opkomen, maar dat het aan de andere kant ook vrijwel aan alle individuele belangen bescherming biedt: van persoonlijke ontplooiing tot geluidsoverlast, van het recht op reputatie tot het recht op eigendom. Bij het recht op gegevensbescherming zijn met name twee punten van belang. Allereerst dient degene die persoonsgegevens verwerkt een legitieme grondslag te hebben. Als het gaat om het verwerken van bijzondere persoonsgegevens, waarmee gevoelige zaken over een persoon duidelijk worden, mag de verwerking in principe niet, tenzij er sprake is van een uitzonderingsgrond op het verwerkingsverbod. Als het gaat om het verwerken van 'gewone' persoonsgegevens kan het ook gaan om een legitiem belang van de verwerkingsverantwoordelijke dat het belang van de betrokkene overstijgt. Daarvan kan sprake zijn bij het maken van camerabeelden op en rond het huis vanwege veiligheidsredenen. In hoeverre dit ook opgaat in het geval van recreatieve doeleinden is niet eenduidig te zeggen en zal van geval tot geval moeten worden beoordeeld. Voor het verwerken van persoonsgegevens met als doel schade of nadeel te berokkenen aan de betrokkene zal vrijwel nimmer kunnen worden vertrouwd op een verwerkingsgrond. Ten tweede gelden er tal van plichten voor de verwerkingsverantwoordelijke. Daarvan is een belangrijk voorbeeld dat als er gegevens over een persoon worden verzameld of verder verwerkt, de betrokkene hier van tevoren over op de hoogte moet worden gesteld. Dit staat het maken van heimelijke opnames of het gebruik van al verzamelde gegevens voor andere doeleinden dan waarvoor ze waren verzameld zonder de betrokkene daar van tevoren in te kennen dus niet toe. Daarnaast moet de verwerkingsverantwoordelijke ook afdoende technische en organisatorische veiligheidsmaatregelen treffen.

7 Strafrecht

Bij veel strafbare gedragingen wordt de privacy van het slachtoffer en diens menselijke waardigheid aangetast. Denk bijvoorbeeld aan delicten als inbraak, verkrachting en mishandeling. In dit overzicht richten wij ons op de 'digitale schendingen' van de horizontale privacy. Met andere woorden, gedragingen zoals beschreven in hoofdstuk 2 die gezien de aard en de omstandigheden als strafwaardig worden bestempeld. Hierbij gaat het primair om delicten 1) gericht op het (heimelijk) observeren en verzamelen van gegevens, 2) uitingsdelicten, 3) delicten gericht tegen de zeden en 4) delicten gericht tegen de persoonlijke vrijheid.

7.1 Heimelijk observeren / verzamelen van gegevens

Delicten die gericht zijn op het heimelijk observeren van personen en het wederrechtelijk verzamelen van gegevens bevinden zich in Titel V van het Wetboek van Strafrecht (misdrijven tegen de openbare orde).

7.1.1 Computervredebreuk (138ab Sr)

Computervredebreuk is de digitale variant van huisvredebreuk. Het binnendringen van een geautomatiseerd werk van een natuurlijk persoon leidt al snel tot een inbreuk op de persoonlijke levenssfeer, met name omdat op smartphones, computers enzovoorts veel privacygevoelige gegevens staan. Denk aan foto's, IM en SMS berichten, emails, agenda's en persoonlijke documenten.

Computervredebreuk is vaak een delict dat tot doel heeft om andere delicten mogelijk te maken zoals bijvoorbeeld het heimelijk overnemen van gegevens. Zo kan nadat eenmaal wederrechtelijk toegang is verkregen tot het geautomatiseerde werk *spyware* worden geïnstalleerd waarmee verdere privacyschendingen plaatsvinden. Op computervredebreuk staat een maximale gevangenisstraf van twee jaar.

7.1.2 Overname gegevens (138c Sr)

Wanneer een persoon wederrechtelijk gegevens overneemt uit een geautomatiseerd werk voor zichzelf of anderen (het kopiëren van gegevens), dan kan deze persoon een maximale gevangenisstraf krijgen van twee jaar.

7.1.3 Afluisteren, aftappen of opnemen van gegevens (Artikel 139c Sr)

Daar waar artikel 138c Sr betrekking heeft op opgeslagen gegevens heeft artikel 139c Sr betrekking op 'stromende gegevens'. Het gaat daarbij om het afluisteren, aftappen of opnemen van gegevens die worden overgedragen (bijvoorbeeld via het internet). Artikel 139d Sr stelt het gebruik van technische hulpmiddelen daartoe strafbaar. De maximale straf is twee jaar gevangenisstraf.

7.1.4 Heimelijk opnemen gesprekken (artikel 139a en 139b Sr)

De artikelen 139a en 139b Sr stellen het opzettelijk heimelijk opnemen van gesprekken strafbaar. Artikel 139a Sr heeft betrekking op het met een technisch hulpmiddel opzettelijk opnemen van een gesprek dat in een woning, besloten lokaal of erf wordt gevoerd. Artikel 139b Sr stelt het elders opnemen van

gesprekken strafbaar. De artikelen 139a en 139b Sr zijn niet van toepassing op het opnemen van gesprekken waaraan je als persoon zelf deelneemt, ook al zijn de gesprekspartners niet op de hoogte van het feit dat het gesprek wordt opgenomen. De maximale gevangenisstraf is respectievelijk drie en zes maanden.

7.1.5 Heimelijk cameratoezicht (139f Sr)

Het gaat bij heimelijk cameratoezicht om het zonder dat kenbaar te maken, opzettelijk en wederrechtelijk filmen van personen.[150] Wanneer heimelijk cameratoezicht wordt toegepast in een woning of andere niet voor het publiek toegankelijke plaats, levert dit het delict zoals beschreven in artikel 139f Sr op. Wanneer het heimelijk cameratoezicht plaatsvindt in de publieke ruimte zonder duidelijke aanduiding dan levert dit de overtreding van artikel 441b Sr op. De maximale gevangenisstraf voor heimelijk cameratoezicht is twee jaar.

7.1.6 Beschikken over en aanbieden van wederrechtelijk verkregen gegevens (139e Sr)

Op het ter beschikking hebben van een voorwerp waarop gegevens zijn vastgelegd die door wederrechtelijk afluisteren, aftappen of opnemen van een gesprek, telecommunicatie of andere gegevensoverdracht of andere gegevensverwerking door een geautomatiseerd werk zijn verkregen, staat een gevangenisstraf van maximaal zes maanden.

7.1.7 Helen / verwerven van wederrechtelijk verkregen gegevens (Artikel 139g Sr)

Naast de strafbaarstellingen aan de 'productie kant', is ook het ontvangen van wederrechtelijk verkregen gegevens strafbaar gesteld. Artikel 139g Sr stelt het bezit van gegevens strafbaar waarbij de bezitter weet of redelijkerwijs had moeten vermoeden dat deze afkomstig zijn uit een misdrijf. De maximale gevangenisstraf bedraagt één jaar.

7.1.8 Creëren, aanbieden en verspreiden van *malware*

Via verschillende artikelen is het creëren, aanbieden en verspreiden van *malware* verboden. Het gaat dan om technische hulpmiddelen die hoofdzakelijk geschikt zijn om: 1) schade toe te brengen aan geautomatiseerde werken en informatie (350d Sr), of 2) computervredebreuk te faciliteren (139d Sr). In artikel 441b Sr is het strafbaar gesteld om malware aan te bieden en aan te prijzen en daarbij de illegale functionaliteiten te benadrukken.

Veel van de technische hulpmiddelen die gebruikt kunnen worden om horizontale privacyschendingen mee te plegen (bijvoorbeeld *stalkerware*) hebben kenmerken van malware. Problematisch is evenwel dat hun primaire doel niet schade toebrengen is of computervredebreuk faciliteren. Het is daarmee niet eenvoudig om een *ex ante* verbod op dit soort hardware en software te construeren op basis van deze bepalingen.

[150] Zie ook EHRM, Grote Kamer, 12 november 2013, zaaknummer 5786/08 (*Söderman v. Zweden*)

7.2 Uitingsdelicten

Uitingsdelicten sanctioneren uitingen waarvan de inhoud strafbaar is. In het kader van het onderwerp van dit onderzoek zijn in het bijzonder de volgende delicten relevant:

7.2.1 Belediging (266 Sr)

Titel XVI van het wetboek van Strafrecht houdt zich bezig met belediging. Artikel 266 Sr betreft de eenvoudige belediging. Elke opzettelijke belediging die niet het karakter van smaad of smaadschrift draagt wordt gekwalificeerd als eenvoudige belediging en gestraft met gevangenisstraf van ten hoogste drie maanden. Het kan gaan om mondelinge beledigingen of beledigingen bij afbeelding of geschrift. Als zodanig vallen beledigingen gedaan in een online omgeving ook binnen de delictsomschrijving.

7.2.2 Smaad en laster (artikel 261 Sr en 262 Sr)

Bij *smaad* is de opzet van de verdachte gericht op het aantasten van de eer en goede naam van het slachtoffer door 'telastlegging' van een bepaald feit, met het oogmerk om daar ruchtbaarheid te geven. Wanneer de smadelijke uiting is gedaan in afbeelding of geschrift, is er sprake van smaadschrift en gaat de maximale gevangenisstraf omhoog van zes maanden naar één jaar. Wanneer het ten laste gelegde feit in strijd met de waarheid is, dan is er sprake van *laster*. In dit geval is de maximale straf twee jaar gevangenisstraf. *Fake news* gericht op het beschadigen van de reputatie van een persoon kan bijvoorbeeld worden gekwalificeerd als laster.

Relevant voor eenvoudige belediging, smaad en laster is dat het klachtdelicten zijn (artikel 269 Sr). Met andere woorden, enkel op aangeven van het slachtoffer volgt strafvervolging.

7.2.3 Groepsbelediging en aanzetten tot haat (137c en 137d Sr)

Iemand die zich in het openbaar, mondeling of bij geschrift of afbeelding, opzettelijk beledigend uitlaat over een groep mensen (bijvoorbeeld wegens hun ras, godsdienst of seksuele gerichtheid) maakt zich schuldig aan groepsbelediging (artikel 137c Sr). Wanneer een dergelijke uiting tot doel heeft om aan te zetten tot haat, discriminatie of gewelddadig optreden, dan is er sprake van haatzaaien (137d Sr). Anders dan titel XVI betreft het hier geen klachtdelict.[151] De artikelen 137e Sr en 137f Sr stellen verschillende vormen van het bijdragen aan uitingsdelicten strafbaar. De maximale gevangenisstraffen zijn respectievelijk één en twee jaar.

7.2.4 Wraakporno (139h Sr)

Artikel 139h Sr stelt diverse vormen van misbruik van seksueel beeldmateriaal strafbaar. Zowel het openbaar maken van heimelijk vervaardigd beeldmateriaal, als beeldmateriaal dat met wederzijdse goedkeuring is gemaakt maar zonder goedkeuring is gedeeld, valt binnen de delictsomschrijving. Hiermee

[151] Vaak zal een belediging tot een enkele persoon op basis van bepaalde groepskenmerken (bijv. 'jij en je soort') zowel kenmerken hebben van een individuele belediging als een groepsbelediging. Het is dan met name relevant wie geadresseerd wordt door de opmerking en in hoeverre anderen (die ook tot de beledigde groep behoren) kennis kunnen nemen van de belediging. Zie in dit kader: Rodrigues, P. R. (2008), Monitor Racisme & Extremisme, 8e rapportage, (red. van Donselaar, J. en Rodrigues, P. R.), Pallas Publications, Amsterdam University Press, p. 244

zijn diverse vormen van grensoverschrijdend seksueel gedrag zoals wraakporno, *upskirting* en voyeurisme strafbaar gesteld.[152]

7.3 Misdrijven tegen de zeden

7.3.1 Afbeelding of voorwerp aanstotelijk voor de eerbaarheid (artikel 240 Sr)

Het ongewild aanbieden van pornografisch materiaal aan een persoon is aanstotelijk voor de eerbaarheid.[153] Met eerbaarheid wordt gedoeld op *'de eerbaarheid als algemeen begrip zoals dat moet worden opgevat naar de hier te lande heersende zeden, welke worden bepaald door de bij een belangrijke meerderheid van het Nederlandse volk op dit punt levende opvattingen'*.[154] Het toezenden van expliciet pornografisch materiaal bijvoorbeeld per email kan een schending van de eerbaarheid opleveren. De maximale gevangenisstraf bedraagt twee maanden.

7.3.2 Bezitten en verspreiden van kinderpornografisch materiaal (artikel 240b Sr)

Kindermisbruik vormt een ernstige aantasting van de lichamelijke integriteit en de menselijke waardigheid en is daarnaast ook een schending van de horizontale privacy, in het bijzonder wanneer de beelden van het misbruik verspreid worden. Het verspreiden, aanbieden, openlijk tentoonstellen, vervaardigen, invoeren, doorvoeren, uitvoeren, verwerven, bezitten en openbaarmaken van kinderpornografisch materiaal is strafbaar gesteld in artikel 240b Sr. De maximale gevangenisstraf is vier jaar. Wanneer de dader van het plegen een beroep of een gewoonte maakt is de maximale gevangenisstraf acht jaar.

7.4 Misdrijven gericht tegen de persoonlijke vrijheid

7.4.1 Bedreiging en afpersing (artikel 284 en artikel 317 Sr)

Een uiting wordt gekwalificeerd als bedreiging wanneer deze tot doel heeft iemand iets (niet) te laten doen of dulden en om dit te bewerkstelligen één van de volgende twee dingen wordt gedaan:

- Iemand bedreigen met geweld of een andere feitelijkheid;
- Wanneer een slachtoffer wordt bedreigd met smaad of smaadschrift.

Een voorbeeld van de tweede situatie is *sextortion,* waarbij gedreigd wordt met de publicatie van seksueel getint materiaal. Relevant hierbij is dat de tweede situatie een klachtdelict betreft, de eerste situatie niet.

Er is sprake van afpersing (317 Sr) als het doel is om door dreiging met geweld het slachtoffer te dwingen om goederen af te staan, schulden aan te gaan, schulden kwijt te schelden of gegevens ter beschikking te

[152] Tweede Kamer, vergaderjaar 2018-2019, 35 080, nr. 3, p. 4
[153] Het artikel volgt op het algemene artikel 239 Sr (schennis van de eerbaarheid) dat echter in de context van dit rapport een beperkte relevantie heeft.
[154] Kool, R. S. B., Tekst & Commentaar Strafrecht, Pornografie bij: Wetboek van Strafrecht, Artikel 240 [Afbeelding of voorwerp aanstotelijk voor de eerbaarheid]; zie ook ECLI:NL:HR:1971:373

stellen. Er is sprake van afdreiging wanneer om wederrechtelijk voordeel te behalen het slachtoffer wordt bedreigd met smaad of smaadschrift. Ook hier kan bij *sextortion* sprake zijn.[155]

De maximale gevangenisstraf voor bedreiging is twee jaar, voor afpersing is het negen jaar.

7.4.2 Belaging (artikel 285b Sr)

Belaging, in de volksmond ook wel *stalking* genaamd, is stelselmatig wederrechtelijk inbreuk op iemands persoonlijke levenssfeer maken. Belaging is dus bij uitstek een delict waarbij de horizontale privacy in het geding is. De belager moet het oogmerk hebben de ander iets te laten doen, dulden of vrees aan te jagen.[156] Of de belager er ook daadwerkelijk in slaagt om het slachtoffer vrees aan te jagen is voor de bewezenverklaring niet direct relevant. Nu de persoonlijke levenssfeer ruim geïnterpreteerd dient worden, kan belaging zich ook (deels) in de online wereld afspelen.[157] Belaging is een klachtdelict. De maximale gevangenisstraf bedraagt drie jaar.

Hoewel stelselmatig en wederrechtelijk inbreuk maken op de persoonlijk levenssfeer met de bedoeling om daarmee iemand te beïnvloeden doorgaans een actieve (zichtbare) inmenging in de persoonlijke levenssfeer vergt, kan er ook sprake zijn van belaging pas nadat iemand op de hoogte is geraakt van de inbreukmakende gedragingen.[158] Ook kan iemand heimelijk filmen als belaging worden gezien aldus de Hoge Raad. Dit omdat door bewust en gedurende langere tijd iemand onopgemerkt filmen, een verdachte bewerkstelligt dat het slachtoffer zich niet kan verzetten en aldus gedwongen wordt dat filmen te dulden.[159]

Een aan belaging gerelateerd delict is 'hinderlijk volgen' (artikel 426bis Sr). Deze overtreding stelt het hinderlijk volgen van een persoon of personen op de openbare weg strafbaar. In de context van digitale privacyschendingen is dit delict evenwel niet relevant, omdat het bestanddeel 'openbare weg' bij online hinderlijk volgen niet te bewijzen valt. De vraag is of een 'online' variant van dit noodzakelijk is, nu - afhankelijk van de omstandigheden van het geval- belaging ook van toepassing kan zijn.

7.4.3 Valsheid in geschrift en oplichting

Onder omstandigheden kan bij het plegen van valsheid in geschrift of oplichting ook sprake zijn van een horizontale privacyschending, bijvoorbeeld wanneer er misbruik wordt gemaakt van iemands identiteit. In Nederland heeft de wetgever er voor gekozen om identiteitsdiefstal niet zelfstandig strafbaar te stellen, omdat deze gedraging 'afgedekt' wordt door bepalingen als valsheid in geschrift (art. 225 Sr), oplichting (326 Sr), of omdat de gedraging in dienst staat van delicten als diefstal, verduistering en heling (artikelen 310, 321 en 416 Sr) die reeds strafbaar zijn gesteld.[160]

---

[155] Cleiren, C. P. M, Ten Voorde, van Waas W. (2019), *Strafbaarstelling van sexchatting en sextortion onder de loep. De meerwaarde van een empirisch perspectief,* Strafblad nummer 2, MEi 2019 / SdU
[156] van der Meij, P. P. J., Tekst & Commentaar Strafrecht, commentaar op art. 285b Sr
[157] Zie bijvoorbeeld: EHRM, 25 september 2001, app. no. 44787/98 (*P.G. and J.H. v. Verenigd Koninkrijk*); EHRM 16 december 1992, app. no. 13710/88 (*Niemitz v. Duitsland*), EHRM, 21 juni 2011, app. no. 30194/09 (*Shimolovos v. Rusland*)
[158] Zie: ECLI:NL:HR:2014:3095
[159] Zie: ECLI:NL:HR:2020:673
[160] de Vries, U.R.M.Th., Tigchelaar, H., van der Linden, M., Hol, A.H. (2007), *Identiteitsfraude een afbakening: een internationale begripsvergelijking en analyse van nationale strafbepalingen*, WODC 1496

In de toekomst zouden ook *deepfakes* gebruikt kunnen worden om personen op te lichten of te misleiden. Naast het delict oplichting komt mogelijk ook valsheid in geschrift in beeld, hoewel het bestanddeel 'geschrift' daartoe zeer ruim geïnterpreteerd moet worden. In de Memorie van Toelichting bij artikel 225 Sr wordt namelijk gesproken over 'in letter- of cijferschrift gestelde stukken'. Een afbeelding op video kan dus niet zonder meer onder deze definitie worden gevangen.[161]

7.5 Rechtsvergelijking

Op basis van het onderzoek in de verschillende landen blijkt dat strafrechtelijke normering van horizontale privacyschendingen redelijk uniform is. In deze paragraaf richten wij ons daarom alleen op de wezenlijke verschillen. Dat wil zeggen, wij bespreken delictsomschrijvingen die wij in Nederland niet kennen, dan wel die delictsomschrijvingen in andere landen die noemenswaardig verschillen van de Nederlandse variant.

7.5.1 Duitsland

Duitsland kent sinds 2014 in paragraaf 201a Strafgesetzbuch een strafbaarstelling van het filmen van personen in een toestand van hulpeloosheid (*Hilflosigkeit*). Het vormt een onderdeel van een bredere strafbaarstelling van inbreuken op de persoonlijke levenssfeer door middel van de vastlegging en verspreiding van beelden. Artikel 201a geeft invulling aan de maatschappelijke wens om de privacy beter te waarborgen.[162] Het artikel is een reactie op de toenemende bedreigingen voor de privacy in de vorm van spycams, drones en het internet als een medium voor de snelle verspreiding van beelden.[163]

Hulpeloosheid heeft een objectief aspect (daadwerkelijke hulpeloosheid) en een subjectief asepct (zichzelf hulpeloos achten). Het onbevoegd maken, doorgeven en/of openbaar maken van beelden van hulpbehoevenden en daarmee hun waardigheid aantasten wordt gestraft met een straf van ten hoogste twee jaar. Voorbeelden van gedragingen die binnen de delictsomschrijving vallen zijn het filmen van slachtoffers van verkeersongelukken, bebloede slachtoffers van geweldsmisdrijven, dronken mensen die onderweg naar huis zijn en dronken tieners.[164] Slaap en ouderdom zijn op zichzelf nog geen hulpeloze toestanden. De ratio achter de bepaling is dat mensen schade kunnen leiden door beelden van situaties waar zij in beland zijn die buiten hun controle liggen. Extra bescherming is geëigend wanneer de hulpeloze toestand niet aan henzelf te wijten is (zoals bijvoorbeeld bij ongelukken of misdrijven), hoewel het voorbeeld van dronkenschap aangeeft dat ook zelf toegebrachte hulpeloosheid beschermenswaardig moet worden geacht.[165]

---

[161] Verheul, J. M., Tekst & Commentaar Strafrecht, Valsheid in geschrift bij: Wetboek van Strafrecht, Artikel 225 (laatst geraadpleegd 26 mei 2020)
[162] Heuchemer, P. (2020), 'StGB § 201a Verletzung Des Höchstpersönlichen Lebensbereichs Durch Bildaufnahmen' in: v Heintschel-Heinegg (ed), *BeckOK StGB* (45th edn, 2020) 4.
[163] Bundestag Drucksache 15/2466, p. 5.
[164] Bundesrat, Stenografischer Bericht, 929. Sitzung, 19 December 2014, 25; Bundestag, Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss), Drucksache 18/3202 (neu), 18. Wahlperiode, 12 November 2014, 28 en Bundestag, Stenografischer Bericht, 67. Sitzung, 14 November 2014, 12.
[165] Bundestag Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss), Drucksache 18/3202 (neu), 18. Wahlperiode, 12 November 2014, 28 en Kühl, K., Heger, M. (2014) Strafgesetzbuch: Kommentar, Beck-Online, StGB §243, Rn. 21.

7.5.2 Polen

In tegenstelling tot Nederland heeft Polen identiteitsfraude als zelfstandig delict strafbaar gesteld in artikel Art. 190a(2) van het Poolse Wetboek van Strafrecht. In Nederland heeft de wetgever er voor gekozen om identiteitsdiefstal niet zelfstandig strafbaar te stellen, omdat deze gedraging zoals gezegd 'afgedekt' wordt door andere delictsomschrijvingen. In Polen is echter een specifieke vorm van identiteitsfraude strafbaar gesteld, namelijk identiteitsfraude met als doel om door het misbruik van deze identiteit de echte persoon te schaden. Vandaar dat deze gedraging ook in hetzelfde artikel is opgenomen als de belaging. In Nederland is deze gedraging als zodanig niet zelfstandig strafbaar. Afhankelijk van de omstandigheden van het geval kan deze gedraging mogelijk wel gevat worden onder bijvoorbeeld belediging of laster, of in ernstige gevallen onder de belaging. Met de komst van *deepfakes* zou de relevantie van een dergelijke bepaling mogelijk kunnen toenemen.

Verder is het interessant om te zien dat in Polen lichtere schendingen van de horizontale privacy niet via het strafrecht maar via het administratief recht worden afgedaan. Het gaat om vergrijpen die niet serieus genoeg zijn om via het strafrecht geadresseerd te worden. Hierbij moet worden gedacht aan het mensen lastig vallen of opzettelijk misleiden om een reactie uit te lokken (artikel 107), het in het openbaar uithalen van 'nare' *practical jokes* of *pranks* en het plaatsen van obscene advertenties, afbeeldingen of teksten in de publieke ruimte. Deze bepalingen zouden van toepassing kunnen zijn op ernstige vormen van *trolling* en cyberpesten in situaties waarin (nog) niet voldaan is aan de criteria voor het delict belaging.[166]

7.5.3 Verenigd Koninkrijk

De strafrechtelijke normering van privacyschendingen in het Verenigd Koninkrijk is ook vergelijkbaar met die in Nederland. Voor de vraagstelling van dit rapport zijn met name sectie 127 van *Communications Act* en de *Malicious Communications Act* interessant.[167] Deze bepalingen zijn interessant omdat ze een brede strafbaarstelling kennen voor het verspreiden van aanstootgevend materiaal. Hiermee fungeren zij als '*catch all*' bepalingen die gebruikt kunnen worden om allerlei horizontale privacyschendingen te criminaliseren in afwezigheid van specifieke regelingen. Sectie 127 van de Communications Act is in het bijzonder relevant en luidt:

"(1) A person is guilty of an offence if he—
(a) sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or
(b) causes any such message or matter to be so sent.

(2) A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he—
(a)sends by means of a public electronic communications network, a message that he knows to be false,
(b)causes such a message to be sent; or

[166] In Italië is specifieke wetgeving aangenomen om cyberpesten te bestrijden. Naast een verbod op cyberpesten op zichzelf zijn er ook specifieke regels die internettussenpersonen dwingen om binnen 48 uur content te verwijderen die door pestkoppen is geplaatst. Zie: *LEGGE 29 maggio 2017, n. 71 Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo.*
[167] *Malicious Communications Act 1988*, 1988 Chapter 27

(c)persistently makes use of a public electronic communications network."

Een voorbeeld waar deze bepaling is toegepast is de veroordeling van een man voor het maken van foto's van een dodelijk slachtoffer van de Grenfell Tower ramp in 2017 en het plaatsen van deze foto's op zijn Facebook pagina.[168] Het tweede lid van sectie 127 kan mogelijk ook worden gebruikt voor de bestrijding van *fake news* en voor (ernstige) vormen van *trolling*. Hoewel een uitzondering voor de pers niet expliciet is genoemd in het artikel, zullen perspublicaties veelal buiten de scope van de bepaling liggen omdat er geen opzet is op het veroorzaken van *'annoyance, inconvenience or needless anxiety'*.

Wraakporno is in het Verenigd Koninkrijk reeds in 2015 strafbaar gesteld via sectie 33 van de *Criminal Justice and Courts Act 2015*.[169] Op het moment van schrijven wordt deze wet geëvalueerd door de *Law Commission* met het oog op mogelijke knelpunten in de toepassing.[170] Knelpunten zijn onder andere de vraag in hoeverre de bepaling kan worden toegepast in het kader van virtuele wraakporno (bijvoorbeeld door middel van *deepfakes*) en het gebrek aan anonimiteit binnen rechtszaken waardoor slachtoffers geen aangifte doen, of aangiftes intrekken. De inzichten uit dit evaluatieproces kunnen ook voor de Nederlandse situatie relevant blijken.

Voor de Nederlandse rechtspraktijk is tenslotte de *Intimidatory Offences Definitive Guideline* uit 2018 nog interessant.[171] In deze richtlijn zijn onder andere strafverzwarende omstandigheden beschreven zoals het opnieuw plaatsen van beelden die eerder offline zijn gehaald of het bewust het oogmerk hebben om het slachtoffer te vernederen.

7.5.4 Zweden

Zweden kent een relatief brede strafbaarstelling van privacyschendingen (*olaga integritetsintrång*) in hoofdstuk 4, sectie 6c van het Zweedse Wetboek van Strafrecht (*Brottsbalken)*. Het gaat om het verspreiden van beelden betreffende iemands seksuele leven, gezondheidstoestand, slachtofferschap van een misdrijf, kwetsbare/hulpeloze toestand of naakte lichaam. Voorwaarde voor strafbaarheid is dat de verspreiding kan resulteren in serieuze schade voor het slachtoffer. De maximale straf is twee jaar gevangenisstraf. De strafbaarstelling is hiermee op hoofdlijnen gelijk aan de strafbaarstelling in Duitsland.

Relevant is ten slotte nog de Zweedse BBS wetgeving.[172] Deze wetgeving die stamt uit 1998 en destijds voor *bulletin board systems* in het leven is geroepen, kent een *revival* omdat de definitie van een bulletin board (een dienst voor de verzending van elektronische berichten) ook van toepassing kan zijn op internetplatformen. Deze wet is relevant, omdat het een verplichting aan houders van *bulletin boards* oplegt om berichten te verwijderen en ontoegankelijk te maken wanneer deze strafbare content bevatten. Hieruit kan een monitoringsplicht voor strafbare content worden afgeleid.

[168] Zie: https://www.bbc.com/news/uk-41314418
[169] http://www.legislation.gov.uk/ukpga/2015/2/contents/enacted
[170] https://www.lawcom.gov.uk/project/taking-making-and-sharing-intimate-images-without-consent/
[171] Sentencing Council (2018), *Intimidatory Offences Definitive Guideline*; via: https://www.sentencingcouncil.org.uk/wp-content/uploads/Intimidatory-offences-definitive-guideline-Web.pdf
[172] *Lag (1998:112) om ansvar för elektroniska anslagstavlor BBS-lagen*

7.6 Afsluitende beschouwing

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.[173] 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. Er wordt gewerkt aan een initiatiefwet om verkeerslachtoffers te beschermen.[174] Het lijkt verstandig een eventuele strafbaarstelling evenwel breder te trekken, in lijn met de Duitse of Zweedse wetgeving op dit gebied. 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 gehouden moeten worden.

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

[173] In Italië is wraakporno ook strafbaar gesteld. Interessant aan de Italiaanse strafbaarstelling is dat het feit dat het verspreiden van seksuele beelden van een partner of ex-partner een strafverzwarende omstandigheid is. Hiermee wordt extra nadruk gelegd op het belang van het beschermen van intieme, vertrouwde relaties. Zie artikel artikel 612-ter *Codice Penale*.
[174] Zie: Tweede Kamer, vergaderjaar 2018–2019, Aanhangsel, 1034

of obscene beelden, in het bijzonder wanneer deze gericht 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. Zo kan *happy slapping* worden aangemerkt als mishandeling en kan het doen van de *blind bird box challenge* in een auto een overtreding van artikel 5 Wegenverkeerswet opleveren.[175]

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 is. Ook bestaat er het gevaar van willekeur in de toepassing. Tenslotte kan (pro-actieve) handhaving een inbreuk op de persoonlijke levenssfeer opleveren.

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.

Het stelselmatig volgen van de locatie van een persoon (bijvoorbeeld door hun GPS-coördinaten te verzamelen met behulp van een peilbaken of geïnstalleerde *stalkerware*) is niet zelfstandig strafbaar gesteld in Nederland en de door ons onderzochte landen. Een dergelijk volgen van iemands gedrag is weliswaar een inbreuk op de persoonlijke levenssfeer, maar wanneer de belager niet het oogmerk heeft om het slachtoffer iets te laten doen, dulden of vrees aan te jagen, dan is er (nog) geen sprake van belaging.[176] Of er hiermee een lacune in de rechtsbescherming bestaat valt te betwijfelen. Het verzamelen van de gegevens zal waarschijnlijk doorgaans op zichzelf een strafbaar feit opleveren (bijvoorbeeld omdat de gegevens zijn verzameld door middel van computervredebreuk), dan wel het verwerken van de gegevens staat in dienst van een ander strafbaar feit zoals belaging.

Tenslotte is het opnemen van gesprekken waaraan je zelf deelnemer bent geen strafbare gedraging. Desalniettemin kan eventuele publicatie daarvan wel als een horizontale privacyschending worden gezien. In het bijzonder wanneer de gesprekpartners niet op de hoogte zijn van het feit dat het gesprek wordt

[175] *Happy slapping* is het filmen van het slaan van argeloze voorbijgangers, de *blind bird box challenge* is het geblinddoekt voltooien van uitdagingen zoals op straat lopen of autorijden.
[176] Wel kan mogelijk analoog aan de uitspraak van Hoge Raad in relatie tot het heimelijk filmen van een persoon worden gesteld dat het niet in staat zijn om de inbreuk tegen te houden gelezen kan worden als het 'moeten dulden'.

opgenomen en het gesprek of delen daarvan openbaar worden gemaakt. Ditzelfde geldt voor conversaties via Instant Messaging. Het is een maatschappelijke vraag of een dergelijke gedraging strafrechtelijk gesanctioneerd moet worden. Wanneer de publicatie van de gegevens de eer of goede naam van het slachtoffer aantast dan biedt het delict smaad uitkomst. Zelfstandige strafbaarstelling kan druk zetten op de vrijheid van meningsuiting en daarnaast biedt het civiel recht mogelijk voldoende waarborgen (de generaal preventieve werking van een mogelijke actie uit onrechtmatige daad na publicatie van vertrouwelijke conversaties).

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.[177] 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.

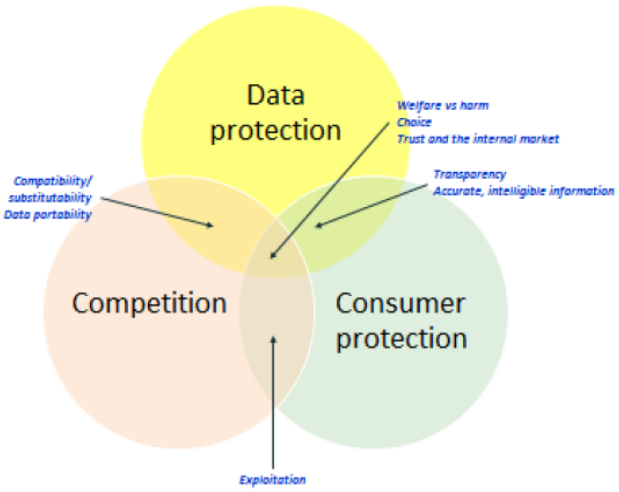
[177] Het aantal geregistreerde misdrijven dat valt onder de delictsomschrijvingen zoals beschreven in dit hoofdstuk ligt rond de 45.000. Het betreft hier een zeer grove schatting omdat de registratie niet op altijd op het niveau van een individueel delict is terug te voeren. Zie: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83648NED/table?ts=1589221899074. Voor deze cijfers is niet terug te vinden hoeveel van deze zaken daadwerkelijk (succesvol) vervolgd zijn.

8 Administratief recht, mededingingswetgeving en consumentenbescherming

Het administratief recht en het mededingingsrecht spelen een beperkte rol bij het reguleren van privacy in horizontale verhoudingen. Toch is een aantal punten in het administratief recht, het mededingingsrecht en bestaande consumentenbescherming van belang. Deze punten worden achtereenvolgens aangestipt, daarbij waar relevant verwijzend naar voorbeelden uit het buitenland. Aan de relatie tussen het gegevensbeschermingsrecht, consumentenrecht en mededingingsrecht is in het verleden al aandacht besteed. Zo heeft de European Data Protection Supervisor er op gewezen dat veel problemen en vraagstukken in de data-gedreven samenleving zich op het snijvlak van deze drie rechtsgebieden bevinden:

"Although privacy and the protection of personal data are public interests and fundamental rights recognised in the Treaties, the lack of interaction in the development of policies on competition, consumer protection and data protection may have reduced both the effectiveness of competition rules' enforcement and the incentive for developing services which enhance privacy and minimise potential for harm to the consumer. In the digital economy personal information represents a significant intangible asset in value creation and a currency in the exchange of online services. This has potentially far-reaching implications for the interpretation of key concepts including transparency, market dominance, and consumer welfare and harm."[178]

Onderstaand beeld is hoe de EDPS de relatie tussen gegevensbescherming, mededingingsrecht en consumentenrecht visualiseert.



Afbeelding 3. Bron: European Data Protection Supervisor 2014

[178] European Data Protection Supervisor (2014), *Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, maart 2014

In dit hoofdstuk zullen wij achtereenvolgens het consumentenrecht (8.1), het mededingingsrecht (8.2) en het administratief recht (8.3) bespreken in relatie tot privacy en gegevensbescherming.

8.1 Consumentenbescherming

Consumentenbescherming biedt burgers bescherming tegen bedrijven, met name als zij hun macht misbruiken of misleidend te werk gaan. Een voorbeeld is de Richtlijn oneerlijke handelspraktijken, waarin een aantal handelspraktijken verboden is.[179] Een oneerlijke handelspraktijk is een praktijk die in strijd is met de vereisten van professionele toewijding, en het economische gedrag van de gemiddelde consument die zij bereikt of op wie zij gericht is of, indien zij op een bepaalde groep consumenten gericht is, het economisch gedrag van het gemiddelde lid van deze groep, met betrekking tot het product wezenlijk verstoort of kan verstoren.[180] De Richtlijn ziet op twee typen oneerlijke handelspraktijken: misleidende en agressieve handelspraktijken. Als misleidend wordt beschouwd een handelspraktijk die gepaard gaat met onjuiste informatie en derhalve op onwaarheden berust of, zelfs als de informatie feitelijk correct is, de gemiddelde consument op enigerlei wijze, inclusief door de algemene presentatie, bedriegt of kan bedriegen en de gemiddelde consument er toe kan brengen een besluit over een transactie te nemen dat hij anders niet had genomen.[181] Als agressief wordt beschouwd een handelspraktijk die, in haar feitelijke context, al haar kenmerken en omstandigheden in aanmerking genomen, door intimidatie, dwang of ongepaste beïnvloeding, de keuzevrijheid of de vrijheid van handelen van de gemiddelde consument met betrekking tot het product aanzienlijk beperkt of kan beperken, waardoor hij ertoe wordt gebracht of kan worden gebracht over een transactie een besluit te nemen dat hij anders niet had genomen.[182]

Een voorbeeld is van een misleidende handelspraktijk wordt in de Richtlijn gegeven: "*Een product als 'gratis', 'voor niets', 'kosteloos' en dergelijke omschrijven als de consument iets anders moet betalen dan de onvermijdelijke kosten om in te gaan op het aanbod en het product af te halen dan wel dit te laten bezorgen.*" Wetenschappers wijzen er op dat alhoewel veel internetdiensten geen betaling in euro's vereisen, de echte betaling geschiedt via persoonsgegevens, ook wel de nieuwe olie genoemd, die in veel gevallen meer waard zijn dan de paar euro's die de gemiddelde burger bereid zou zijn te betalen voor een internetdienst.[183] Daarnaast is het ook verboden je als handelaar niet als zodanig bekend te maken; ook daarvan zou sprake kunnen zijn bij internetplatformen die zich niet zozeer presenteren als commerciële bedrijven die hun eigen belang nastreven, maar doen alsof zij er voor de belangen van de gebruikers zijn en soms zelfs claimen het publiek belang te dienen.

Daarnaast wijst de European Data Protection Supervisor in haar opinie over privacy, big data en mededinging nog op een aantal andere richtlijnen die mogelijkerwijs van belang kunnen zijn:

[179] Richtlijn 2005/29/EG Van het Europees Parlement en de Raad van 11 mei 2005 betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt en tot wijziging van Richtlijn 84/450/EEG van de Raad, Richtlijnen 97/7/EG, 98/27/EG en 2002/65/EG van het Europees Parlement en de Raad en van Verordening (EG) nr. 2006/2004 van het Europees Parlement en de Raad (Richtlijn Oneerlijke Handelspraktijken)
[180] Artikel 5 Richtlijn Oneerlijke Handelspraktijken
[181] Artikel 6 Richtlijn Oneerlijke Handelspraktijken
[182] Artikel 8 Richtlijn Oneerlijke handelspraktijken
[183] Zie bijvoorbeeld: https://www.njb.nl/blogs/je-geld-of-je-gegevens/

"The Directive on Unfair Contract Terms therefore introduced the notion of 'good faith' and required contract terms to be drafted in plain and intelligible language, with any doubt about the meaning of a term to be interpreted in favour of the consumer. Under the Price Indication Directive traders are required to provide the selling price in a way that is easily identifiable and clearly legible. The Consumer Rights Directive goes further in its aim to eliminate hidden charges and costs in 'off-premises' transactions, particularly those over the internet, such as where individuals are deceived into paying for services presented as 'free'. It requires traders to inform customers in a 'clear and comprehensible manner' of the 'total price of the goods or services… or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated….' (Article 6 (e)). More specifically traders are required to provide information on the content of digital services such as their compatibility with hardware and software."[184]

De eerstgenoemde richtlijn kan in het geding zijn als bedrijven lange en onduidelijke contracten voorleggen aan consumenten die zij redelijkerwijs niet kunnen worden geacht te begrijpen of die hen onevenredig veel tijd zou kosten om te doorgronden. Prijsindicaties kunnen ook misleidend zijn, zoals toegelicht.

Ook kan worden gewezen op de Richtlijn inzake productveiligheid.[185] Producenten zijn volgens de richtlijn gehouden uitsluitend veilige producten op de markt te brengen. Het is de vraag of de apparatuur en software die op de markt wordt gebracht waarmee gegevens kunnen worden verzameld en verwerkt, zoals allerhande *Internet of Things* producten, aan deze standaard voldoen aangezien vele niet of nauwelijks beveiligd zijn. Als een beveiligingscamera die wordt opgehangen ter beveiliging van een huis of gebouw eenvoudig gehackt kan worden en daarmee in wezen tot meer onveiligheid leidt – bijvoorbeeld omdat dieven kunnen zien of de eigenaren van een huis thuis zijn – dan is het de vraag of aan deze richtlijn wordt voldaan.[186]

Tot slot kan in het kader van het consumentenrecht worden gewezen op contractuele bepalingen. Er is veel te doen geweest over de vraag in hoeverre de overeenkomsten die burgers met internetbedrijven sluiten rechtsgeldig zijn, onder meer omdat het de vraag is of zij:

1) vrij zijn in hun keuze (kan een puber van 14 realistisch gezien zonder Instagram, TikTok en Facebook?);
2) begrijpen wat de gevolgen zijn van hun keuze (zeker als het gaat om de toekomstige verdere verwerking van hun gegevens voor andere doeleinden);

---

[184] European Data Protection Supervisor (2014), *Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*. Zie verder: Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts; Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers; Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council
[185] Richtlijn 2001/95/EG van het Europees Parlement en de Raad van 3 december 2001 inzake algemene productveiligheid
[186] Zie voor eventuele aansprakelijkheid van producenten hoofdstuk 10

3) onderkennen dat de werkelijke overeenkomst ziet op een ruil tussen de aangeboden dienst en hun persoonsgegevens en
4) de waarde van hun eigen gegevens kennen (wat mogelijk tot een vorm van dwaling zou kunnen leiden).

Daarmee is het de vraag in hoeverre een dergelijke overeenkomst voldoet aan de voorwaarden die daaraan worden gesteld in boek drie van het Burgerlijk Wetboek en of een dergelijke overeenkomst nietig dan wel vernietigbaar is. Daarnaast is ook gewezen op de Europese Principes van het Contract Recht, waarin onder meer is vervat:

"Contract terms which have not been individually negotiated may be invoked against a party who did not know of them only if the party invoking them took reasonable steps to bring them to the other party's attention before or when the contract was concluded. Terms are not brought appropriately to a party's attention by a mere reference to them in a contract document, even if that party signs the document."[187]

De vraag is in hoeverre de manier van verwijzingen naar de *Terms and Conditions* en het *Privacy Statement* door bedrijven in de internetomgeving aan de test van *'appropriateness'* voldoet.

8.2 Mededingingsrecht

Het mededingingsrecht heeft als doel machtsconcentraties en machtsmisbruik te voorkomen. Deze uitgangspunten kunnen indirect doorwerken in horizontale verhoudingen, omdat veel privacyschendingen worden gepleegd via of met behulp van digitale internetdiensten en internetplatformen.

Het mededingingsrecht volgt onder meer uit Artikel 102 van het Verdrag voor de Werking van de Europese Unie. Daarin is vervat:

"*Onverenigbaar met de interne markt en verboden, voor zover de handel tussen lidstaten daardoor ongunstig kan worden beïnvloed, is het, dat een of meer ondernemingen misbruik maken van een machtspositie op de interne markt of op een wezenlijk deel daarvan. Dit misbruik kan met name bestaan in: a) het rechtstreeks of zijdelings opleggen van onbillijke aan- of verkoopprijzen of van andere onbillijke contractuele voorwaarden; b) het beperken van de productie, de afzet of de technische ontwikkeling ten nadele van de verbruikers; c) het toepassen ten opzichte van handelspartners van ongelijke voorwaarden bij gelijkwaardige prestaties, hun daarmede nadeel berokkenend bij de mededinging; d) het feit dat het sluiten van overeenkomsten afhankelijk wordt gesteld van het aanvaarden door de handelspartners van bijkomende prestaties, welke naar hun aard of volgens het handelsgebruik geen verband houden met het onderwerp van deze overeenkomsten.*"[188]

Het mededingingsrecht heeft tot een aantal gezichtsbepalende zaken geleid in de digitale omgeving. In 2004 beschikte de Europese Commissie ten aanzien van Microsoft bijvoorbeeld dat Microsoft

[187] Zie: Europese Principes van het Contract Recht, bepaling 2:104, via: https://www.trans-lex.org/400200/_/pecl/#head_24
[188] Verdrag betreffende de werking van de Europese Unie. Zie ook: Verordening (EG) Nr. 1/2003 van de Raad van 16 december 2002 betreffende de uitvoering van de mededingingsregels van de artikelen 81 en 82 van het Verdrag. Verordening (EG) Nr. 139/2004 van de Raad van 20 januari 2004 betreffende de controle op concentraties van ondernemingen (de „EG-concentratieverordening")

bedrijfsinformatie moest vrijgeven en het gebruik ervan toe moest staan voor de ontwikkeling van compatibele producten. Ook mocht Microsoft geen beperkingen opleggen met betrekking tot het soort producten waarin de specificaties geïmplementeerd mochten worden, indien daardoor de stimulans om met Microsoft te concurreren, werd afgezwakt of de mogelijkheden van de begunstigden om te innoveren, onnodig werden ingeperkt. Ten slotte dienden de door Microsoft in de toekomst opgelegde voorwaarden voldoende voorspelbaar te zijn.[189] Deze beschikking bleef voor het Europees Hof van Justitie grotendeels in stand.[190]

Ook tegen Google is het mededingingsrecht een aantal keer ingezet. Zo oordeelde de Europese Commissie in 2017 dat Google haar eigen prijsvergelijkingsdienst een prominentere plaats en betere weergave op haar algemene zoekresultatenpagina's gaf en daardoor verkeer weghaalt bij concurrerende prijsvergelijkingsdiensten.[191] In 2018 bepaalde de Commissie onder meer dat het bedrijf zich schuldig maakte aan koppelverkoop van de Google Search-app, koppelverkoop van Google Chrome en het feit dat aan betalingen uit hoofde van portfolio-gebaseerde inkomstendeling de voorwaarde werd verbonden dat geen concurrerende algemene zoekdienst werd voorgeïnstalleerd. Er werd een boete van meer dan vier miljoen euro opgelegd.[192] In 2019 kwam de Commissie tot de conclusie dat:

"*Google minstens sinds 2006 een machtspositie heeft op de EER-markt voor intermediatiediensten bij onlinezoekadvertenties. Dit komt met name door de zeer hoge marktaandelen van Google – voor het grootste deel van deze periode meer dan 85 %. De markt wordt ook gekenmerkt door hoge toetredingsdrempels. Daarbij gaat het onder meer om zeer hoge initiële en lopende investeringen die nodig zijn om algemene zoektechnologie te ontwikkelen en te onderhouden, een platform voor zoekadvertenties, en een voldoende ruim portfolio van zowel publishers als adverteerders. Google heeft deze machtspositie op de markt misbruikt door concurrenten te beletten op de markt voor intermediatiediensten bij onlinezoekadvertenties te concurreren.*"[193]

Daarvoor werd een boete van anderhalf miljoen euro opgelegd.

Als interessant buitenlands voorbeeld kan worden gewezen op de beslissing van het Duitse Bundeskartellamt ten aanzien van Facebook. Het Amt constateerde dat Facebook een dominante marktpositie had op het gebied van online sociale media en dat deze macht werd misbruikt:

---

[189] Beschikking van de Commissie van 24 mei 2004 betreffende een procedure overeenkomstig artikel 82 van het EG-Verdrag en artikel 54 van de EER-Overeenkomst tegen Microsoft Corporation (Zaak COMP/C-3/37.792 – Microsoft) (Kennisgeving geschied onder nummer C(2004) 900)

[190] Arrest van het Gerecht van eerste aanleg (Grote kamer) van 17 september 2007. Microsoft Corporation tegen Commissie van de Europese Gemeenschappen. Zaak T-201/04.

[191] Samenvatting van het besluit van de Commissie van 27 juni 2017 inzake een procedure op grond van artikel 102 van het Verdrag betreffende de werking van de Europese Unie en artikel 54 van de EER-overeenkomst (Zaak AT.39740 – Google Search (Shopping)) (2018/C 9/08)

[192] Samenvatting van het besluit van de Commissie van 18 juli 2018 inzake een procedure op grond van artikel 102 van het Verdrag betreffende de werking van de Europese Unie en artikel 54 van de EER-overeenkomst (Zaak AT.40099 – Google Android) (Kennisgeving geschied onder document C(2018) 4761) (2019/C 402/08)

[193] Samenvatting van het besluit van de Commissie van 18 juli 2018 inzake een procedure op grond van artikel 102 van het Verdrag betreffende de werking van de Europese Unie en artikel 54 van de EER-overeenkomst (Zaak AT.40099 – Google Android) (Kennisgeving geschied onder document C(2018) 4761) (2019/C 402/08)

"The extent to which Facebook collects, merges and uses data in user accounts constitutes an abuse of a dominant position. The Bundeskartellamt's decision is not about how the processing of data generated by using Facebook's own website is to be assessed under competition law. As these data are allocated to a specific service users know that they will be collected and used to a certain extent. This is an essential component of a social network and its data-based business model. However, this is what many users are not aware of: Among other conditions, private use of the network is subject to Facebook being able to collect an almost unlimited amount of any type of user data from third party sources, allocate these to the users' Facebook accounts and use them for numerous data processing processes. Third-party sources are Facebook-owned services such as Instagram or WhatsApp, but also third party websites which include interfaces such as the "Like" or "Share" buttons. Where such visible interfaces are embedded in websites and apps, the data flow to Facebook will already start when these are called up or installed. It is not even necessary, e.g., to scroll over or click on a "Like" button. Calling up a website with an embedded "Like" button will start the data flow. Millions of such interfaces can be encountered on German websites and on apps. Even if no Facebook symbol is visible to users of a website, user data will flow from many websites to Facebook. This happens, for example, if the website operator uses the "Facebook Analytics" service in the background in order to carry out user analyses."[194]

In hoger beroep heeft het Oberlandesgericht Düsseldorf echter besloten dat ook al zou er sprake zijn van een overtreding van de AVG, dit niet automatisch betekent dat Facebook ook misbruik maakt van haar dominante marktpositie.[195] Om die reden werd de uitspraak van het Amt door het Oberlandesgericht opgeschort. Op 23 juni 2020 heeft de Kartellsenat van het Bundesgerichtshof echter het oordeel van het Oberlandesgericht teruggedraaid. Het Bundesgerichtshof is van mening dat het wel degelijk mogelijk is voor Facebook om haar dominante marktpositie te misbruiken om via haar gebruiksvoorwaarden gegevensverwerkingen af te dwingen en daarmee de privacy van de gebruikers te schenden.[196]

In Nederland heeft de Autoriteit Consument en Markt (ACM) zich nog slechts in beperkte mate gericht op de digitale multinationals zoals Facebook, Apple, Google en Microsoft. Wel heeft het, in samenwerking met andere Europese consumententoezichthouders Facebook zover gekregen een aantal aanpassingen te doen aan de algemene voorwaarden.[197] In een eerder stadium heeft de voorloper van de ACM, de Nederlandse Mededingingsautoriteit (NMA), een klacht van de Consumentenbond tegen Apple afgewezen. Alhoewel de Consumentenbond stelde dat Apple misbruik maakte van haar machtspositie op de markten voor draagbare muziekspelers en voor online muziekwinkels door koppelverkoop van iPod en iTunes, meende de NMA dat consumenten muziekbestanden van iTunes kunnen en mogen afspelen op een andere draagbare muziekspeler dan de iPod. Verder kunnen en mogen consumenten muziekbestanden die van een andere online winkel dan iTunes zijn verkregen met een iPod afspelen. De NMA liet daarbij in het midden of er sprake was van een economische machtspositie evenals de specifieke marktafbakening, omdat het door de Consumentenbond vermeende misbruik niet vastgesteld werd.[198]

[194] Zie: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html
[195] Zie: http://www.justiz.nrw.de/nrwe/olgs/duesseldorf/j2019/Kart_1_19_V_Beschluss_20190826.html
[196] https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html?nn=10690868
[197]Zie: https://www.acm.nl/nl/publicaties/overzicht-toezeggingen-aanpassing-algemene-voorwaarden-facebook
[198] Zie: https://www.acm.nl/nl/publicaties/publicatie/2036/Besluit-op-klacht-consumentenbod-machtspositie-Apple

8.3 Administratief recht

Het algemeen administratief recht is als zodanig van beperkt belang in horizontale verhoudingen. Wel kan het een rol spelen bij de handhaving en naleving van bepaalde normen. Een voorbeeld daarvan is dat veel Algemene Plaatselijke Verordeningen regels stellen die zien op de bescherming van onderlinge privacy. Zo bepaalt de APV van Amsterdam:

'Het is verboden bewakingsapparatuur te gebruiken wanneer daarmee personen kunnen worden waargenomen in een ander gebouw, vaartuig of besloten erf dan waar de bewakingsapparatuur staat opgesteld. Het is verboden zich op of aan de weg op te houden met de kennelijke bedoeling personen die zich op of aan de weg of in een gebouw of vaartuig bevinden te bespieden.'[199]

Daarnaast verbiedt de APV ook geluidsoverlast en hinderlijk gedrag. Daarvan kan bijvoorbeeld sprake zijn bij het geval van drones die geluidshinder veroorzaken en over de heg in de achtertuin kunnen kijken. Alhoewel een deel van de bepalingen in APV's strafrechtelijk van aard zijn, worden de regels primair bestuursrechtelijk gehandhaafd. Vandaar dat de APV's in deze paragraaf worden besproken.

Bij de APV geldt met name het vraagstuk van handhaving. Een buitengewoon opsporingsambtenaar (BOA) kan moeilijk iedere drone in de stad achtervolgen om te kijken wie de eigenaar is, of er opnames van de openbare ruimte of van privéruimtes zijn gemaakt en of dit legitiem en volgens de wet is geschied. Een probleem zal in toenemende mate zijn, zoals in een eerder hoofdstuk uitgelegd, dat producten waarmee burgers elkaars onderlinge privacy kunnen schenden goedkoper worden, wijder verbreid raken en kleiner worden of geïntegreerd in alledaagse producten. Daarmee zal het steeds lastiger worden om basale regels en open normen te handhaven door overheidsdiensten en functionarissen.

Dat geldt in het klein voor BOAs, maar in het groot net zo goed voor handhavende organisaties als de Autoriteit Persoonsgegevens. Ook voor de AP is het ondoenlijk om bij alle *smartphones*, *drones*, *IoT devices* en andere soft- en hardware waarmee burgers elkaars privacy zouden kunnen schenden na te gaan of dit inderdaad is gebeurd en als een inbreuk wordt geconstateerd, hierop te acteren. Zelfs als dit mogelijk zou zijn is het sterk de vraag of dit wenselijk is. Een overheidsinstantie die burgers zo dicht op de huid zit is vermoedelijk een remedie die erger is dan de kwaal. Daarom wordt momenteel met name gehandhaafd op extreme gevallen; alledaagse inbreuken die onrechtmatig zijn maar niet direct tot grote schade leiden zullen grotendeels ongeadresseerd blijven (zo is veel gebruik van drones momenteel verboden, maar wordt het gebruik daarvan oogluikend toegestaan).

Dit wijst op een meer algemeen punt ten aanzien van horizontale privacy. Veelal is de normstelling duidelijk, maar is de handhaving gebrekkig. Daarbij is de keuze tussen Scylla en Charybdis, tussen handhaving via het civielrecht, waarbij burgers primair zelf als belanghebbende moeten opkomen tegen acties die hen schade hebben berokkend, terwijl zij vaak noch de benodigde kennis noch de middelen noch de expertise hebben om dergelijke rechtszaken te voeren, én handhaving door overheidspartijen,

[199] Via: https://decentrale.regelgeving.overheid.nl/cvdr/xhtmloutput/Historie/Amsterdam/CVDR72510/CVDR72510_32.html

waarbij de benodigde middelen en mankracht ontbreken, maar het ook de vraag is of het wenselijk is om een overheidsorganisatie alledaags gebruik van digitale technologieën en détail te laten controleren.

8.4 Afsluitende beschouwing

Het consumentenrecht richt zich op de bescherming van consumenten, die als zwakkere partij worden gezien. Zo worden burgers met name in 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 en zijn grote internetbedrijven als Facebook, Microsoft en Google aangepakt vanwege onder meer misbruik van hun monopoliepositie en koppelverkoop.

Niet voor niets heeft onder meer de European Data Protection Supervisor gewezen op het feit dat in Big Data processen vaak sprake zal zijn van een samenloop van gegevensbeschermingsrecht, consumentenbeschermingsrecht en mededingingsrecht. Daarom heeft het opgeroepen tot meer samenwerking tussen de bestuursrechtelijke overheidsorganen die toezien op de naleving van deze rechtsgebieden: in Nederland zijn dat de Autoriteit Persoonsgegevens en de Autoriteit Consument en Markt. Ook speelt bestuursrechtelijke handhaving een rol op lokaal niveau, onder meer bij de Algemene Plaatselijke Verordening die regels stelt ten aanzien van hinderlijke gedrag en de schending van de onderlinge privacy.

De vraag daarbij is in hoeverre het realistisch is dat deze drie rechtsgebieden in horizontale verhoudingen een grote rol zullen spelen; eerder lijkt het voor de hand te liggen dat ze diagonale relaties 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.

Tot slot moet nog het volgende worden opgemerkt. Er is in dit hoofdstuk uitgegaan van een onderscheid tussen publieke instanties en algemene belangen enerzijds en private organisaties en burgers en particuliere belangen anderzijds. Alhoewel dit onderscheid nog steeds een kernuitgangspunt is van het vigerende juridische stelsel moet tegelijkertijd worden opgemerkt dat er ook vele tussenvormen zijn, die laveren tussen beide zijden. Juist deze tussenvormen zullen van essentieel belang zijn in de 21ste eeuw. Enerzijds gaat het dan om publieke organisaties die voor burgers en hun belangen opkomen. Een voorbeeld hiervan is uiteraard de Autoriteit Persoonsgegevens, maar ook de Autoriteit Consument en Markt kan voor consumentenbelangen opkomen. De zaken die worden gevoerd om de marktmacht en feitelijke monopolies van internetgiganten te beteugelen dienen indirect ook private belangen. Een ander voorbeeld zijn burgerrechtenorganisaties, zoals Amnesty International, Bits of Freedom en Privacy First, die rechtszaken voeren in het algemeen belang. Een recent voorbeeld daarvan in de zaak omtrent het SyRI-programma van de overheid. Tot slot kan worden gewezen op de mogelijkheid om collectieve belangen te beschermen en klachten van honderden en soms zelfs duizenden getroffenen als gevolg van eenzelfde feit te bundelen en in één rechtszaak te behandelen. Een recent onderzoek voor het WODC heeft dan ook met name op dit punt de verschillende mogelijkheden voor versterking van het Nederlands recht besproken. Dat werd noodzakelijk geacht in verband met het veranderende informatielandschap. Uit die studie bleek dat het nationale en supranationale procesrecht zich momenteel kenmerken door een sterke

focus op de bescherming van de belangen van individuele rechtssubjecten in de concrete omstandigheden van het geval. Die nadruk werkt goed voor veel traditionele rechtsgeschillen: een bouwvergunning die wordt afgewezen, een verzoek om schadevergoeding na een lasterlijke publicatie of een beperking van privacy door de overheid, waarbij iemands telefoon voor een bepaalde periode wordt afgetapt of iemands huis wordt binnengetreden door de politie. Daarbij is de mogelijke inbreuk immers beperkt tot een specifiek persoon of een kleine groep, is de eventuele schending in tijd en ruimte af te bakenen en is het belang dat op het spel staat individueel en duidelijke bepaalbaar. Dat ligt echter anders bij moderne mensenrechtenvraagstukken die draaien om grote gegevensverzamelingsprocessen, zo concludeerde het onderzoek.

'Big Data projecten zijn nauwelijks in tijd, ruimte en persoon af te bakenen, maar vormen een structureel en voortdurend onderdeel van de handelingen en gedragingen van overheidsdiensten, bedrijven en burgers. De camera's op de hoek van vrijwel iedere straat in de grote steden hebben bijvoorbeeld geen specifiek effect op één bepaald individu, ze filmen permanent eenieder die zich in de stad begeeft; een inlichtingendienst die de communicatiegegevens van een hele wijk of een stad verzamelt raakt niemand specifiek of individueel, maar iedereen gelijkelijk; de politie die door gebruikmaking van predictive policing in bepaalde wijken meer surveilleert dan in andere brengt daarmee geen schade toe aan concrete individuen, maar het kan wel de ongelijkheid in de samenleving in stand houden of zelfs versterken. Hoe groter de dataverwerkingsprocessen en hoe algemener de verzamelde gegevens, des te moeilijker zal het zijn voor een individu om zijn belang concreet te maken. In wezen gaat het bij dit soort Big Data-processen vaak niet om de bescherming van individuele belangen, maar om algemene belangen. Willen we een samenleving waarin de publieke ruimte constant wordt gemonitord en waarin instanties op burgers mogen experimenteren met gedragsbeïnvloeding? Wat zouden rechtsstatelijke waarborgen moeten zijn tegen het gevaar van machtsmisbruik door overheidsdiensten die veel data mogen verzamelen en welke mate van democratische legitimatie dienen dergelijke gegevensverzamelingen te hebben? Welke gevolgen heeft het personaliseren van onder meer verzekeringen en socialezekerheidsrechten voor de solidariteit in de samenleving en het draagvlak voor het spreiden van risico's?'[200]

Daarom is in die studie uitgebreid stilgestaan bij de mogelijkheden om het Nederlands recht met name op het punt van collectieve en algemene belangen(acties) te versterken, onder meer door consequenties te verbinden aan bias in informatiesystemen die binnen het strafrecht worden gebruikt, het versterken van de positie van burgerrechtenorganisaties in het civiel- en bestuursrecht, het introduceren van *amicus curiae* participatie, breder mogelijk maken van het toetsen van algemeen verbindende voorschriften en het oprichten van een proefprocessenfonds.

[200] van der Sloot, B, van Schendel S. (2019), *De Modernisering van het Nederlands Procesrecht in het licht van Big Data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving*, WODC 2019

9 Civiel recht

Het algemeen persoonlijkheidsrecht vindt in Nederland zijn oorsprong in het civiel recht. Lindenbergh stelt dat de algemene persoonlijkheidsrechten kunnen worden beschouwd als de *"civielrechtelijke variant van grondrechten of mensenrechten."*[201] Verhey stelt in zijn proefschrift dat er een tendens is grondrechten *indirect* te laten doorwerken in het civiel recht.[202]

Door de horizontale werking van grondrechten (in het bijzonder artikel 8 EVRM) en het door de Hoge Raad geformuleerde algemeen persoonlijkheidsrecht kan het recht op privacy worden betrokken in een belangenafweging in civiele zaken, zonder dat dit een directe toetsing aan de Nederlandse grondwet vereist. Het is bijvoorbeeld mogelijk de maatschappelijke betamelijkheid van artikel 6:162 BW nader in te vullen met het recht op privacy.[203]

9.1 Onrechtmatige daad

In het civiel recht vormt het leerstuk van de onrechtmatige daad het belangrijkste kader voor de normering van horizontale privacyschendingen. Een schending van de privacy in horizontale privacy verhoudingen kan een onrechtmatige daad opleveren, bijvoorbeeld omdat daarmee de eer en goede naam van een persoon wordt aangetast, of omdat de benadeelde de controle over zijn of haar persoonsgegevens heeft verloren.

De schade als gevolg van een horizontale privacyschending kan zowel materieel als immaterieel zijn. Daar waar het gaat om andere schade dan vermogensschade kan een schadevergoeding op grond van artikel 6:106 BW worden afgedwongen. Zo kan een benadeelde voor een schadevergoeding in aanmerking komen wanneer deze *"in zijn eer of goede naam is geschaad of op andere wijze in zijn persoon is aangetast."* Hiervoor moest worden aangetoond dat de benadeelde geestelijk letsel had opgelopen.[204] In het *EBI* arrest heeft de Hoge Raad echter meer ruimte gecreëerd om tot een schadevergoeding te komen. De Hoge Raad overwoog:

"(…) het op andere wijze in de persoon aangetast zijn van artikel 6:106 lid 1 sub b, slot BW vereist hetzij geestelijk letsel, dan wel een (zeer) ernstige normschending en gevolgen'."[205]

Een ernstige normschending (zoals bijvoorbeeld een schending van het grondrecht op privacy) geeft dus aanspraak op schadevergoeding.

[201] Lindenbergh, S. D. (1999), De Positie en Handhaving van Persoonlijkheidsrechten in het Nederlandse Privaatrecht, in: *Tijdschrift voor Privaatrecht*, pp. 1665–1707
[202] Verhey, L. (1992), *Horizontale werking van grondrechten, in het bijzonder het recht op privacy*, Tjeenk Willink
[203] Alberdingk Thijm, C. (2000), *Privacy versus auteursrecht in een digitale omgeving*, ITER reeks, p. 36.
[204] Engelhard, E. (2019), *Ruimer baan voor smartengeld bij inbreuken op fundamentele rechten? Een reactie op HR 15 maart 2019, ECLI:NL:HR:2019:376*, via: http://blog.ucall.nl/index.php/2019/03/ruimer-baan-voor-smartengeld-bij-inbreuken-op-fundamentele-rechten-een-reactie-op-hr-15-maart-2019-eclinlhr2019376/
[205] Hoge Raad, 15 maart 2019, ECLI:NL:HR:2019:376 (*EBI arrest*)

In 2019 was het de Rechtbank Overijssel die als eerste deze ruimte gebruikte om tot een schadevergoeding te komen voor een overtreding van de AVG.[206] De Rechtbank overwoog:

"6. Voor nadeel dat niet uit vermogensschade bestaat, heeft een benadeelde overeenkomstig artikel 6:106 van het Burgerlijk Wetboek (BW) recht op een naar billijkheid vast te stellen schadevergoeding indien de benadeelde in zijn eer of goede naam is geschaad of op andere wijze in zijn persoon is aangetast. De wetgever heeft daarbij het oog gehad op geestelijk letsel dat bestaat uit ernstige inbreuken op de persoonlijke levenssfeer of op andere persoonlijkheidsrechten van de betrokkene."[207]

In casu ging het om het verspreiden van persoonsgegevens aan derden die geen legitieme basis hadden voor de ontvangst van deze gegevens. Hierdoor verloor de eiser de controle over zijn persoonsgegevens. In hoger beroep oordeelde de Afdeling Bestuursrechtspraak van de Raad van State dat een onrechtmatige verwerking van persoonsgegevens weliswaar kan resulteren in (im)materiële schade en dat een betrokkene daartoe een vergoeding moet krijgen, maar dat dit niet betekent dat elke normschending per definitie tot schade leidt.[208] De eiser zal moeten onderbouwen waaruit de schade bestaat, tenzij er sprake is van een dusdanig ernstige normschending dat nadelige gevolgen daarvan voor de benadeelde zo voor de hand liggen, dat een aantasting in de persoon kan worden aangenomen.[209] Ook onderstreept de Afdeling dat de schadevergoeding op grond van de AVG geen punitief karakter heeft. Het doel is niet om de normovertreder leed toe te voegen maar de daadwerkelijk geleden schade te vergoeden.[210]

De AVG geeft betrokkenen die materiële of immateriële schade hebben geleden ook een recht op schadevergoeding van de verwerkingsverantwoordelijke of de verwerker die de schade heeft veroorzaakt (artikel 82 lid 1 AVG). In zoverre het gaat om horizontale verhoudingen kan dan via een civielrechtelijke actie de schadevergoeding worden afgedwongen. Hierbij is het voor de betrokkene ook mogelijk om zich te laten vertegenwoordigen door bijvoorbeeld een stichting. Deze kan namens een grotere groep betrokkenen een procedure voeren.

Wanneer er sprake is van een horizontale privacyschending waarbij een derde partij een rol speelt (zoals bijvoorbeeld een internetplatform) en de betrokkene wil deze derde partij op grond van de AVG aanspreken, dan moet deze partij als verwerkingsverantwoordelijke kunnen worden aangemerkt. Op grond van de jurisprudentie van het EHvJ kunnen internetplatformen als (mede)verantwoordelijke voor de verwerking van persoonsgegevens worden aangemerkt.[211] Op grond van de AVG kan deze derde partij dan worden aangesproken voor de vergoeding van de schade.[212] Wel stelt artikel 2 lid 4 AVG dat de AVG geen afbreuk doet aan het regime van de Richtlijn elektronische handel, in het bijzonder met betrekking tot de aansprakelijkheid van internettussenpersonen. Dit impliceert dat wanneer de

[206] Overigens verwijst de Rechtbank niet expliciet naar het arrest, maar veeleer naar de bedoelingen van de wetgever zoals vastgelegd in de overwegingen bij de AVG.
[207] ECLI:NL:RBOVE:2019:1827
[208] Afdeling Bestuursrechtspraak Raad van State, zaaknummer 201905087/1/A2, 1 april 2020, ECLI:NL:RVS:2020:899
[209] Zie: Afdeling Bestuursrechtspraak Raad van State, zaaknummer 201901006/1/A2, 1 april 2020, ECLI:NL:RVS:2020:898, r.o 32
[210] Gesteld kan worden dat leedtoevoeging de taak is van de Autoriteit Persoonsgegevens.
[211] Zie bijvoorbeeld EHvJ, 5 juni 2018, zaaknummer C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*)
[212] Engelhard, E.F.D. (2019), Immateriële schade als gevolg van data-inbreuken: het ondergeschoven kindje van de AVG, in: *Nederlands Tijdschrift voor Burgerlijk Recht*, volume 9/10, pp. 192 - 200

verwerkingsverantwoordelijke internettussenpersoon binnen de vrijwaring valt, een schadevergoeding op grond van een overtreding van een norm uit de AVG niet mogelijk is.

9.1.1 Rectificatie (artikel 6:167 BW)

Wanneer er sprake is van een onrechtmatige publicatie, dan kan op basis van artikel 6:167 BW de benadeelde persoon de rechter verzoeken degene die de uiting gepubliceerd heeft deze te rectificeren.[213]

9.2 Auteursrecht

Het auteursrecht speelt ook een rol bij het beschermen van privacy in horizontale verhoudingen. Voor alle werken die gemaakt zijn door een persoon geldt dat deze de exclusieve exploitatierechten heeft (verveelvoudiging en openbaarmaking). Dit biedt bescherming in die situaties waarin er sprake is van de verspreiding van materiaal (foto's, video's, teksten) die door het slachtoffer zelf zijn gemaakt. Denk hierbij bijvoorbeeld aan erotisch getinte *selfies* die zonder de toestemming van de maker worden verspreid. Hoewel dit mogelijk ook een strafbaar feit oplevert, is het niet gezegd dat het ook in alle gevallen leidt tot een strafrechtelijke vervolging. Het auteursrecht biedt dan een alternatieve mogelijkheid tot het staken van de privacyschending. Wanneer de benadeelde niet degene is die het werk heeft gemaakt, maar bijvoorbeeld degene die de privacy schendt, dan is een actie niet mogelijk, omdat de betrokkene dan niet de rechthebbende is.

9.2.1 Portretrecht

Het auteursrecht beschermt het portret van een persoon, ook al is het werk waarin dit portret is vastgelegd niet door de geportretteerde vervaardigd. In feite vormt het portretrecht een beperking op het auteursrecht. Op grond van artikel 21 Auteurswet is het niet toegestaan om een portret van een persoon openbaar te maken voor zover een redelijk belang van de geportretteerde zich tegen de openbaarmaking verzet. De rechthebbende (degene die het portret heeft gemaakt) moet dit belang wegen en substantiëren waarom het belang van publicatie zwaarder weegt dan de belangen van de geportretteerde. Wanneer een portret in opdracht van een geportretteerde is gemaakt, dan is voorafgaande aan de openbaarmaking toestemming van de geportretteerde nodig. Het portretrecht is geen intellectueel eigendomsrecht, maar een beperking op het auteursrecht ter bescherming van de geportretteerde tegen onrechtmatige schending van zijn recht op privacy of andere met de publicatie van het portret geschonden belangen. Schending van het portretrecht is daarmee een species van de gewone onrechtmatige daad.[214]

9.3 Collectieve procedures

Nederland kent sinds 1994 de mogelijkheid tot het voeren van collectieve procedures. Gedupeerden kunnen zich laten vertegenwoordigen door een belangenorganisatie in een gezamenlijke procedure. Sinds 1 januari 2020 is met de *Wet Afwikkeling van massaschade in een collectieve actie* ook de mogelijkheid ontstaan om een collectieve schadevergoeding op te leggen. Hierdoor is het voor gedupeerden niet langer nodig om nog zelfstandig de schade te claimen die in een eerder stadium is vastgesteld door de rechter in een collectieve actie.

[213] Zie eerder paragraaf 5.3
[214] Rb Rotterdam 30 juli 2008, ECLI:NL:RBROT:2008:BD9665

Collectieve procedures kunnen een belangrijk middel zijn voor slachtoffers die niet individueel hun rechten kunnen of durven halen. Zo voert de stichting Stop Online Shaming bijvoorbeeld namens slachtoffers procedures om privacyschendingen te staken.[215] In juli van dit jaar kondigde de Consumentenbond aan een collectieve actie tegen Facebook te starten wegens het schenden van de privacy van Facebook gebruikers.[216]

De belangenorganisatie zelf kan geen schadevergoeding ontvangen. Wel is het mogelijk om de volledige proceskosten vergoed te krijgen. Dit is echter niet mogelijk voor organisaties die op ideële gronden procederen, zoals de vaststelling dat er een inbreuk op de privacy is gemaakt. Dit vormt een drempel voor het voeren van procedures tegen zowel de overheid als het bedrijfsleven voor vermeende privacyschendingen.[217]

9.4 Rechtsvergelijking

9.4.1 Duitsland

Artikel 823 van het Bürgerliches Gesetzbuch (BGB) biedt benadeelden van een onrechtmatige daad (*Unerlaubte Handlung*) een aanspraak (*Anspruch*) op schadevergoeding van de pleger. Daarnaast kan een benadeelde verwijdering eisen (*Beseitigingsanspruch*) of herroeping (*Widerrufanspruch*) en de rechter een dwangbevel te laten uitspreken om de onrechtmatige handelingen te staken (*Unterlassungsanspruch*). In zoverre wijkt het Duitse recht niet veel af van het Nederlandse burgerlijk recht. Wel anders is dat naast de algemene onrechtmatige daadsactie het Duitse recht in artikel 824 BGB ook een specifieke aanspraak kent in het geval de reputatie van een persoon wordt aangetast door het verspreiden van onwaarheden en dit een gevaar voor de financiële positie van een persoon met zich meebrengt (*Kreditgefährdung*). De eer en de goede naam worden hier als zodanig dus niet direct beschermd, het gaat meer om de financiële positie van een persoon.[218]

9.4.2 Polen

In het Poolse Burgerlijk Wetboek worden persoonlijke goederen / persoonlijkheidsrechten expliciet erkend in artikel 23. Artikel 24 beschrijft de mogelijkheden om een actie in te stellen. Het gaat om het staken van de inbreuk, het terugdraaien van de gevolgen en het vergoeden van eventueel geleden schade.

Daarnaast erkent de Poolse auteurswet (*Ustawa o prawie autorskim*) in artikel 81 het portretrecht. Zonder toestemming is het verspreiden van iemands beeltenis niet toegestaan. Uitzonderingen zijn de verspreiding van beelden van bekende personen of situaties waarin het portret van iemand een onderdeel van een breder beeld (bijvoorbeeld iemand tussen winkelend publiek).

[215] Zie: https://stoponlineshaming.org
[216] Zie: https://www.consumentenbond.nl/acties/facebook/aanmelden
[217] Voor een uitgebreide discussie over innovaties in het procesrecht zie: van der Sloot, B, van Schendel S. (2019), De Modernisering van het Nederlands Procesrecht in het licht van Big Data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving, WODC 2019
[218] Wagner (2017), 'BGB § 824 Kreditgefährdung', in: *Münchener Kommentar zum BGB* (7th edn, 2017) 3.

9.4.3 Verenigd Koninkrijk

Het Engelse gewoonterecht kent 'inbreuk op de privacy' niet als een onrechtmatige daad op zichzelf.[219] De bescherming van het recht op privacy in horizontale verhoudingen is gebaseerd op een lappendeken van gewoonterecht en zelfregulerende instrumenten. Horizontale privacyschendingen kunnen leiden tot acties op basis van 1) *breach of confidence*, 2) *misuse of private information*, 3) *malicious falsehood,* 4) *tort of intentionally causing harm* en 5) *private nuisance*.

Breach of confidence

Er is sprake van een *breach of confidence* wanneer vertrouwelijke informatie wordt gedeeld. In *Coco v. A. N. Clark* werd een driestappen toets voor het vaststellen van een *breach of confidence* geïntroduceerd.[220] De vereisten voor een *breach of confidence* zijn:

- De informatie heeft een vertrouwelijk karakter.[221]
- Het is toevertrouwd aan degene die het vertrouwen schendt op een wijze die vertrouwelijkheid impliceerde.[222]
- De openbaarmaking leidt tot schade voor degene die de informatie aan de ander heeft toevertrouwd.

In tegenstelling tot bijvoorbeeld het gegevensbeschermingsrecht vallen ook mondelinge uitingen onder de bescherming.

Misuse of private information

Bij een actie op grond van *misuse of private information* ligt de nadruk op de gevolgen die de publicatie heeft voor de betrokkene in plaats van op het geschonden vertrouwen.[223] Voor een geslaagde actie moet de benadeelde een redelijke verwachting hebben met betrekking tot de privacy van de gegevens.[224] In *Vidal Hall v. Google* bepaalde de Engelse Supreme Court dat misbruik van persoonsgegevens een onrechtmatige daad kan zijn en dat wanneer daardoor 'distress' is ontstaan bij de betrokkene deze immateriële schade vergoed dient te worden.[225]

Malicious falsehood

Malicious falsehood betreft het toeschrijven van niet gedane uitingen aan een persoon. In tegenstelling tot laster hoeft een aantasting van iemands eer of goede naam niet te worden bewezen.[226]

Tort of intentionally causing harm

---

[219] Brüggemeier, G, Colombi Ciacchi, A., O'Calllaghan, P. (2010), *Personality Rights in European Tort Law (The Common Core of European Private Law) 1st Edition*, Cambridge University Press, p. 25
[220] *Coco v A.N. Clark (Engineers) Ltd* [1969] RPC 41, 47.
[221] *Mosley v. News Group*; cf *PJS & YMA v MGN* [2016] UKSC 26 (a claim of misuse of private information)
[222] *Douglas v. Hello!* [2005] EWCA Civ 595
[223] Campbell v Mirror Group Newspapers Ltd [2004] UKHL 22, PJS v News Group Newspapers Ltd [2016] UKSC 26
[224] Campbell v Mirror Group Newspapers Ltd [2004] UKHL 22
[225] Vidal-Hall v, Google Inc ([2015] EWCA Civ 311)
[226] *Kaye v Robertson* [1991] FSR 62 CA

Wanneer uitingen zijn gericht op het moedwillig schade toebrengen aan een persoon, dan kan een actie op grond van onrechtmatige daad worden ingesteld. De zelfstandige werking van deze actie lijkt beperkt omdat er weinig situaties zijn waarin er niet ook sprake is van smaad of laster.[227] Daar waar het gaat om feitelijk correcte uitspraken zal doorgaans de vrijheid van meningsuiting zwaarder wegen.

Private nuisance
Een laatste mogelijkheid betreft de *tort of private nuisance*. In 2020 oordeelde de Court of Appeal dat door de bouw van een bezoekersgalerij die uitkeek op een aantal appartementen de privacy van de bewoners geschaad werd.[228]

9.4.4 Zweden
Het Zweedse recht kent geen specifiek Burgerlijk Wetboek. Daar waar het gaat om aansprakelijkheidsrecht bestaat er een hybride systeem van jurisprudentie en een specifieke wet betreffende de aansprakelijkheid (de *Skadeståndslag)* uit 1972.[229] Hoewel schade toegebracht aan personen (*personskada*) kan leiden tot aansprakelijkheid is er wel een belangrijke beperking daar waar het gaat om horizontale privacyschendingen. Aansprakelijkheid ontstaat alleen wanneer de schade ontstaan is als gevolg van een handeling die strafbaar is gesteld.[230] Civiele persoonlijkheidsrechten worden in het Zweedse recht niet onderkend.[231] Dit beperkt de mogelijkheden voor benadeelden om op grond van het privaatrecht op te treden tegen horizontale privacyschendingen. De Zweedse wetgeving inzake de vrijheid van de meningsuiting en de vrije pers uit 1776 kent de vergrijpen belediging (*förolämpning*) en laster (*förtal*). Wanneer uitgevers zich hieraan schuldig maken, dan kan de benadeelde een schadevergoedingsactie instellen tegen deze uitgever.

9.5 Afsluitende beschouwing
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, de eiser moet aantonen dat er sprake is van schade, dan wel er moet sprake zijn van een dusdanig ernstige normschending dat nadelige gevolgen daarvan voor de benadeelde zo voor de hand liggen, dat een aantasting in de persoon kan worden aangenomen.[232]

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

[227] *Rhodes v OPO* [2015] UKSC 32
[228] *Fearn and Ors v The Board of Trustees of the Tate Gallery* [2020] EWCA Civ 104
[229] Skadeståndslag (1972:207)
[230] Brüggemeier, G, Colombi Ciacchi, A., O'Calllaghan, P. (2010), *Personality Rights in European Tort Law (The Common Core of European Private Law) 1st Edition*, Cambridge University Press, p. 29
[231] Ibid. p. 29
[232] Zie: ECLI:NL:RVS:2020:898, r.o 32

worden opgetreden tegen horizontale privacyschendingen zoals bijvoorbeeld het verbieden van voorgenomen onrechtmatige perspublicaties, zal vaak op voorhand niet duidelijk zijn dat een burger een privacyschending gaat plegen. Dan resteert de actie uit onrechtmatige daad om eventuele schade te vergoeden. Ook het aanspreken van internetplatformen om pro-actief op te treden is problematisch (zie hoofdstuk 10).

De tweede beperking ligt in de mogelijkheden voor de benadeelde om daadwerkelijk zijn of haar recht te halen.[233] 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. Vaak betekent het eerst een procedure tegen een internetplatform of andere dienstverlener alvorens de daadwerkelijke verweerder in rechte aangesproken kan worden. 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 (namelijk die waar er daadwerkelijk meerdere slachtoffers zijn die gezamenlijk één partij aanspreken).

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 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.

[233] Zie in dit kader ook: van der Sloot, B., Schendel (2019), *De Modernisering van het Nederlands Procesrecht in het licht van Big Data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving,* WODC Projectnummer 2900

10 Aansprakelijkheid van producenten, distributeurs en (internet)tussenpersonen

In dit hoofdstuk kijken we naar de partijen die (indirect) een rol spelen bij het mogelijk maken van horizontale privacyschendingen: de producenten en distributeurs van producten en diensten waarmee de privacy geschonden kan worden en (internet)tussenpersonen via wiens platform horizontale privacyschendingen kunnen worden gepleegd. Hierbij besteden we in het bijzonder aandacht aan de aansprakelijkheid van deze partijen voor horizontale privacyschendingen die burgers onderling plegen.

10.1 Aansprakelijkheid van producenten en distributeurs

Het is de vraag in hoeverre fabrikanten en distributeurs van producten waarmee inbreuk kan worden gemaakt op de privacy hier verantwoordelijkheid voor dragen. Denk bijvoorbeeld aan de fabrikanten van *drones* of *spycams*.

Een producent kan op grond van art. 6:185 lid 1 BW aansprakelijk worden gesteld voor schade veroorzaakt door een gebrek in zijn product. Een product is gebrekkig indien het niet de veiligheid biedt die men er van mag verwachten (6:186 BW). Dit kan bijvoorbeeld het geval zijn wanneer een drone door een technisch mankement plotseling neerstort of ergens tegenaan vliegt en letsel- of zaakschade veroorzaakt. [234] Volgens art. 6:188 BW dient de benadeelde de schade, het gebrek en het oorzakelijke verband tussen het gebrek en de schade te bewijzen. Het gaat dus om schade die ontstaat bij normaal gebruik, waarbij de veiligheid van het product door het toedoen van de producent te wensen overlaat. Wanneer het product 'deugdelijk' is en de schade is ontstaan door de verkeerde aanwending van het product bestaat er in beginsel geen aansprakelijkheid voor de producent.[235] Wel dient de producent de gebruiker te informeren over de (veiligheids)kenmerken van een product. Tot de 'presentatie van het product' behoren waarschuwingen of symbolen ten behoeve van een veilig gebruik. Waarschuwingen die een producent aanbrengt op zijn product kunnen derhalve bepalend zijn voor de aansprakelijkheid van de producent.[236]

Een product kan schade veroorzaken omdat het op verkeerde wijze wordt gebruikt. Indien dit verkeerd gebruik voorzienbaar is, is het aannemelijk dat een producent hiervoor had moeten waarschuwen. In het *Lekkende Kruik* arrest overweegt de HR dat een producent er rekening mee dient te houden dat een deel van het publiek waarvoor het product bestemd is, het nemen van de noodzakelijke voorzorgsmaatregelen zal nalaten.[237] Een producent moet daarom bij het ontwerp en de presentatie van het product de informatievoorziening afstemmen op de 'gemiddelde onvoorzichtige gebruiker'.[238] Er moet bij die onvoorzichtigheid nog wel een link zijn te vinden met het gebrek van het product: de schade moet zijn

[234] Art. 6:190 BW; Custers, B. (2018), Aansprakelijkheid voor drones, in: *Maandblad voor Vermogensrecht* 2018, nummer 7-8, p. 238.
[235] Of gebrekkige beveiliging kan leiden tot aansprakelijkheid voor de fabrikant hangt af van de omstandigheden van het geval. Zie in dit kader: https://zoek.officielebekendmakingen.nl/kst-26643-477.html
[236] Pape, S. (2006), De betekenis van het Jetblast-arrest voor de waarschuwing in het productaansprakelijkheidsrecht, in: *NTBR* 2006, 56, p. 374-382.
[237] HR 2 februari 1973, NJ 1973, 315, m.nt. HB. (*Lekkende kruik I*)
[238] Pape, S. (2006), De betekenis van het Jetblast-arrest voor de waarschuwing in het productaansprakelijkheidsrecht, in: *NTBR* 2006, 56, p. 374-382.

ingetreden als gevolg van de gebrekkigheid (in de presentatie) van een product en niet door het eigen onzorgvuldige gedrag van een gebruiker.

Op grond van het bovenstaande lijkt aansprakelijkheid voor het gebruik van producten die worden gebruikt bij horizontale privacyschendingen daarmee uitgesloten. Eenzelfde beeld zien wij ook terug in de landen uit de rechtsvergelijking. Dit kan waarschijnlijk mede verklaard worden vanuit het feit dat productaansprakelijkheidsregels via het Unierecht zijn geharmoniseerd.

Mogelijk kan het op de markt brengen van een product dat voor horizontale privacyschendingen wordt aangewend nog maatschappelijk onbetamelijk zijn en daarmee onrechtmatig, maar ook dit zal naar ons oordeel niet snel kunnen worden aangenomen.

10.2 Aansprakelijkheid van (internet)tussenpersonen

Veel horizontale privacyschendingen vinden plaats op het internet, bijvoorbeeld via sociale media. De tussenpersonen die de communicatie verzorgen (*access providers*, *hosting providers* en *social media* platformen) 'faciliteren' daarmee indirect horizontale privacyschendingen. De vraag rijst daarmee in welke mate deze tussen internettussenpersonen verantwoordelijk kunnen worden gehouden voor het faciliteren van deze horizontale privacyschendingen. Het valt te verwachten dat wanneer internettussenpersonen eerder aansprakelijk zijn voor het handelen van hun gebruikers, zij een actievere rol nemen in het bestrijden van horizontale privacyschendingen.

Uitgangspunt tot op heden in de wet is dat internettussenpersonen niet aansprakelijk zijn voor het onrechtmatig handelen van gebruikers, zolang zij aan de voorwaarden voldoen zoals gesteld in artikel 6:196c BW, de Nederlandse implementatie van de Richtlijn elektronische handel (Reh).[239] De aansprakelijkheidsbeperkingen ex. artikel 6:196c BW zijn gecodificeerd in een tijd waarin platformen zoals Facebook en Twitter nog niet bestonden. Hoewel de aansprakelijkheidsbepalingen techniek-onafhankelijk zijn geformuleerd, zijn zij desalniettemin geïnspireerd op het toenmalige technologische landschap. In dit landschap bestonden de twee primaire vormen van internetdienstverlening uit *access* (internettoegangsdiensten) en *hosting* (opslag van gegevens ten behoeve van derden).

Voor een *access provider* geldt dat deze niet aansprakelijk is voor onrechtmatig handelen van gebruikers wanneer deze:

- niet het initiatief tot het doorgeven van de informatie neemt;
- niet degene is die bepaalt aan wie de informatie wordt doorgegeven; en
- hij de doorgegeven informatie niet heeft geselecteerd of gewijzigd.

Voor *hosting providers* en internetplatformen geldt dat zij niet aansprakelijk zijn zolang:

[239] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ("Richtlijn inzake elektronische handel")

- zij geen weet hebben van de activiteit of informatie met een onrechtmatig karakter en, in geval van een schadevergoedingsvordering, niet redelijkerwijs behoren te weten van de activiteit of informatie met een onrechtmatig karakter, dan wel
- zodra zij dat weten of redelijkerwijs behoren te weten, prompt de informatie verwijderen of de toegang daartoe onmogelijk maken.

internettussenpersonen zijn op grond van artikel 15 Reh niet gehouden hun dienstverlening pro-actief te monitoren. Echter, van hen mag wel worden verwacht dat zij met de maatschappelijk betamelijke zorgvuldigheid handelen bij de uitvoer van hun dienstverlening.[240] Dit kan – afhankelijk van de omstandigheden van het geval – betekenen dat een tussenpersoon maatregelen moet nemen om te voorkomen dat onrechtmatige uitingen online verschijnen. Hierbij speelt met name een rol in hoeverre het platform een actieve rol speelt bij de onrechtmatige handelingen, dan wel wetenschap heeft (of zou moeten hebben) van de onrechtmatige handelingen op haar platform.[241]

10.2.1 Reikwijdte aansprakelijkheidsvrijwaringen

In de loop der jaren zijn nieuwe vormen van internetdienstverlening ontstaan, waarbij voor privacy in horizontale verhoudingen in het bijzonder de internetplatformen relevant zijn. De vraag is in hoeverre dit aansprakelijkheidsregime ook van toepassing is op internetplatformen en zo ja, onder welke omstandigheden.

Het eerste deel van deze vraag is door het EHvJ bevestigend beantwoord in onder de arresten *L'Oréal v. eBay* en *Sabam v. Netlog*.[242] Omdat internetplatforms gegevens voor hun gebruikers opslaan, kwalificeren zij als *hosting providers* in de zin van artikel 14 Reh. Het antwoord op het tweede deel van de vraag is een stuk ingewikkelder. Dit is afhankelijk van de vraag in hoeverre internetplatformen voldoen aan het in artikel 14 Reh gestelde criterium dat een hostingpartij 1) géén wetenschap mag hebben van de informatie op haar servers, dan wel 2) niet redelijkerwijs behoort te weten van de activiteit of informatie met een onrechtmatig karakter (in het geval van een schadevergoedingsvordering).

Wil een tussenpersoon in aanmerking komen voor de aansprakelijkheidsvrijwaring op grond van de artikel 12 tot en met 14 Reh (artikel 6:196c BW), dan mag zij geen wetenschap hebben van het onrechtmatige karakter van de informatie op haar servers. Uitgangspunt hierbij is dat op het moment dat je als tussenpersoon je niet actief met de inhoud bemoeit, er geen sprake is van wetenschap. Alleen wanneer je er zelf achter komt dat onrechtmatige handelingen plaatsvinden, of een derde je daar op wijst (een *notice*), dan is er sprake van wetenschap.

[240] Zie bijvoorbeeld: Rechtbank Amsterdam, 11 november 2013, C/13/665397 / KG ZA 19-455 MDvH/MB, ECLI:NL:RBAMS:2019:8415
[241] Zie ook: Gerechtshof Amsterdam, 6 december 2016, 200.097.924/01, ECLI:NL:GHAMS:2016:5221 en Hoge Raad, 5 april 2019, 17/01135, ECLI:NL:HR:2019:503 (prejudiciële vragen over de reikwijdte van de aansprakelijkheidsbeperking ex. artikel 14 Reh).
[242] Europees Hof van Justitie, zaaknummer C-324/09, 12 juli 2011 (*L'Oreal v eBay*), ECLI:EU:C:2011:474; Europees Hof van Justitie, zaaknummer C-360/10, 16 februari 2012 (*Sabam v. Netlog*), ECLI:EU:C:2012:85

In het arrest *L'Oréal v. eBay* verduidelijkte het Europees Hof van Justitie het criterium 'actieve bemoeienis'.[243] Het Hof overwoog dat een dienstverlener gebruik kan maken van de aansprakelijkheidsvrijwaring wanneer deze zich beperkt tot *"een neutrale levering van die dienst met behulp van een louter technische en automatische verwerking van de gegevens die hem door zijn klanten zijn verstrekt"*.[244] Wanneer de dienstverlener een actieve rol heeft waardoor hij kennis heeft van of controle over de gegevens, dan is de aansprakelijkheidsvrijwaring niet meer van toepassing. Of er sprake is van actieve bemoeienis hangt dus sterk samen met de aard van de dienstverlening en de mate waarin de aanbieder betrokken is bij het aanbieden van de content. In het geval van eBay ging het om het bieden van bijstand aan klanten om de advertenties te optimaliseren of deze aanbiedingen te bevorderen. Hiermee verloor eBay haar aansprakelijkheidsvrijwaring. Dit in tegenstelling tot dochterbedrijf Marktplaats dat gezien de aard van haar bedrijfsmodel wél van de aansprakelijkheidsvrijwaring gebruik kon maken aldus het Gerechtshof Leeuwarden.[245] Het Hof Leeuwarden oordeelde dat Marktplaats een neutrale positie tussen de verkoper en de kopers innam en zich daarom kon beroepen op de vrijwaring.[246]

Naast de jurisprudentie van het Europees Hof van Justitie is ook de jurisprudentie van het EHRM in relatie tot aansprakelijkheid relevant. Het EHRM stelde in *Delfi v. Estland* vast dat een nieuwssite die ruimte biedt voor commentaar, een actieve rol speelt met betrekking tot de inhoud en als zodanig niet per definitie gevrijwaard hoeft te blijven van aansprakelijkheid.[247] Het Hof overwoog:

"The Chamber shares the opinion of the Court of Appeal that the activities of the defendant in publishing the comments are not merely of a technical, automatic and passive nature. The objective of the defendant is not merely the provision of an intermediary service. The defendant has integrated the comments section into its news portal, inviting visitors to the website to complement the news with their own judgments [hinnangud] and opinions (comments)."

Deze zaak is met het oog op de bescherming van horizontale privacy in het bijzonder relevant, omdat veel schendingen van de horizontale privacy plaatsvinden via dit soort platformen. Zeker wanneer er sprake is van het direct oproepen van gebruikers om bepaalde (onrechtmatige) handelingen te verrichten via het platform, kan aansprakelijkheid worden aangenomen.[248]

In hoeverre bij sociale media platformen zoals Twitter en Facebook sprake is van actieve bemoeienis, dan wel het feit dat zij hadden moeten weten van het onrechtmatige gedrag, is nog niet eenduidig vastgesteld in de rechtspraak. In principe bieden sociale media platformen een neutrale dienst aan. Anders dan bijvoorbeeld in *Delfi*, roepen zij gebruikers bijvoorbeeld niet op om commentaar te geven op door hen geschreven berichten. Wel kan gesteld worden dat zij zich -afhankelijk van het type platform- zich tot op zekere hoogte met de inhoud bemoeien. Zo cureren veel platformen -al dan niet met behulp van algoritmen- inhoud voor hun gebruikers (welke berichten krijgen zij bijvoorbeeld gepresenteerd en welke

[243] EHvJ, 12 juli 2011, zaaknummer C-324/09, (*L'Oreal v eBay*), ECLI:EU:C:2011:474
[244] Ibid., overweging 113
[245] Gerechtshof Leeuwarden, 22 mei 2012 (*Marktplaats v. Stokke*), ECLI:NL:GHLEE:2012:BW6296
[246] Supra 144, Overweging 115
[247] EHRM, 16 juni 2015, app. no. 64569/09 (*Delfi v. Estland*)
[248] Zie in dit kader bijvoorbeeld: Rechtbank Utrecht, 26 mei 2009 (*Brein v. Mininova*), ECLI:NL:RBUTR:2009:BJ6008

niet). Ook *targeten* veel platformen advertenties op gebruikers op basis van hun voorkeuren en interesses. Hiermee hebben deze platformen dus wel een zekere mate van wetenschap van wat de gebruikers doen.

Vooralsnog lijken sociale media platformen zoals Facebook volgens de Europese rechter géén actieve bemoeienis hebben met de inhoud zoals die door gebruikers wordt geplaatst.[249] Wel heeft Facebook actieve bemoeienis met de advertenties die zij plaatst bij de berichten van gebruikers aldus de rechtbank Amsterdam. De voorzieningenrechter oordeelde dat het verwijderen van advertenties waarin de naam en beeltenis van een bekende Nederlander werden gebruikt om een oplichtingspraktijk te ondersteunen de verantwoordelijkheid is van het platform (*in casu* Facebook):

"Het bieden van een platform voor dergelijke advertenties, althans het niet prompt verwijderen daarvan en/of het niet treffen van in redelijkheid te verlangen maatregelen om de verschijning ervan te voorkomen, komt in strijd met de in acht te nemen maatschappelijke zorgvuldigheid en kan daarom in beginsel ook op zichzelf als onrechtmatig handelen jegens [eiser] worden aangemerkt waardoor deze reputatieschade wordt veroorzaakt."[250]

De rechter verwierp hierbij het verweer van Facebook dat zij een neutrale dienst levert:

"Vooralsnog wordt geoordeeld dat aan die voorwaarde, zeker in het geval van de nepadvertenties dat thans voorligt, waarin het gaat om Facebook als exploitant van advertentieruimte, en niet zozeer om Facebook als neutraal communicatieplatform, niet is voldaan. (…) Facebook is in deze rol niet neutraal, zij bepaalt immers door controle op de advertenties, vastgelegd in het hiervoor onder 2.3 aangehaalde Advertentiebeleid, mede de inhoud daarvan en speelt daarin een actieve rol. Dat dit beleid wordt uitgevoerd door middel van een grotendeels geautomatiseerd proces, doet daaraan niet af."[251]

Met betrekking tot het aanbieden van advertenties is Facebook dus in ieder geval niet aan te merken als een neutraal platform aldus de voorzieningenrechter. Een antwoord op de vraag of internetplatformen zoals Facebook die content selecteren voor hun gebruikers (bijvoorbeeld door algoritmisch voorgestelde berichten) zich bemoeien met de inhoud, blijft vooralsnog echter uit.

10.2.2 Welke maatregelen mogen worden verwacht van een tussenpersoon?

Wanneer een tussenpersoon wetenschap heeft van onrechtmatige content dan moet deze onverwijld de onrechtmatige content ontoegankelijk maken of verwijderen. In de praktijk wordt dit meestal aangeduid met de term *notice and takedown*. In de afgelopen twintig jaar zijn de beperkingen van het *notice and takedown* systeem aan de kaak gesteld, met name door auteursrechthebbenden. Het voornaamste bezwaar is dat gebruikers snel de gewraakte content weer online kunnen krijgen. Een ander probleem is dat content tegenwoordig zo snel 'viraal gaat' dat zelfs bij onverwijld handelen van de tussenpersoon de schade al gedaan is door de razendsnelle verspreiding van de content.

[249] Zie: EHvJ 2019, 3 okotber 2019, zaaknummer, C18/18 (*Glawischnig-Piesczek v Facebook Ireland*), ECLI:EU:C:2019:821
[250] Rechtbank Amsterdam, 11 november 2019, C/13/665397 / KG ZA 19-455 MDvH/MB, ECLI:NL:RBAMS:2019:8415
[251] Ibid.

De vraag rijst daarmee in hoeverre van een tussenpersoon mag worden verwacht dat deze (pro-actieve) maatregelen neemt om onrechtmatige content te weren. Uitgangspunt van de Richtlijn Elektronische handel is dat een tussenpersoon geen algemene verplichting heeft om informatie te monitoren (artikel 15 Reh). Wel kan een rechter een maatregel opleggen aan een tussenpersoon.

In *Sabam v. Netlog* oordeelde het EHvJ dat een nationale rechter weliswaar een maatregel kan opleggen aan een provider om pro-actief onrechtmatige content te verwijderen, maar enkel wanneer het een proportionele maatregel betreft.[252] *In casu* ging het om de verplichting voor een sociale media site om auteursrechtelijke beschermde werken van haar platform te weren door middel van de installatie van een filter systeem. Het Europees Hof van Justitie stelde dat de richtlijnen 2004/48/EG, 2001/29/EG en 2000/31/EG samen gelezen en uitgelegd tegen de achtergrond van de vereisten die voortvloeien uit de bescherming van de toepasselijke grondrechten, aldus moeten worden uitgelegd dat zij eraan in de weg staan dat een hostingdienstverlener door een nationale rechter wordt gelast een filtersysteem te installeren:

- voor de informatie die de gebruikers van zijn diensten op zijn servers opslaan;
- dat zonder onderscheid op al die gebruikers wordt toegepast;
- dat preventief werkt;
- dat uitsluitend door hem wordt bekostigd, en
- dat geen beperking in de tijd kent.

In de zaak *Sabam v. Scarlet* kwam het Hof tot een vergelijkbare uitkomst, maar dan voor access providers.

Een voorbeeld van een door het EHvJ proportioneel geachte maatregel is te vinden in het arrest *UPC Telekabel Wien v. Constantin Film Verleih*.[253] Het ging *in casu* om de vraag of een filterings- en blokkeringsmaatregel proportioneel kan zijn. Het Hof stelde dat:

"De door het Unierecht erkende grondrechten moeten aldus worden uitgelegd dat zij niet eraan in de weg staan dat een internetprovider bij rechterlijk bevel wordt verboden om zijn klanten toegang te verschaffen tot een website waarop beschermde werken zonder toestemming van de rechthebbenden online worden geplaatst, wanneer dit bevel niet preciseert welke maatregelen deze internetprovider moet nemen en niet aangeeft dat laatstgenoemde kan ontkomen aan dwangsommen wegens schending van dit bevel door aan te tonen dat hij alle redelijke maatregelen heeft genomen."

Wel stelde het Hof een dubbele voorwaarde aan dergelijke maatregelen, namelijk:

1. De genomen maatregelen mogen internetgebruikers niet nodeloos de mogelijkheid ontzeggen om zich rechtmatig toegang tot de beschikbare informatie te verschaffen; en
2. de maatregelen moeten tot gevolg hebben dat niet-toegestane oproepingen van de beschermde werken worden verhinderd of minstens bemoeilijkt en zij internetgebruikers die

[252] EHvJ, zaaknummer C-360/10, 16 februari 2012 (*Sabam v. Netlog*), ECLI:EU:C:2012:85
[253] EHvJ, zaaknummer C-70/10, 24 november 2011 (*UPC Telekabel Wien v. Constantin Film Verleih*), ECLI:EU:C:2011:771

gebruikmaken van de diensten van de adressaat van dat bevel ernstig ontraden om zich toegang te verschaffen tot deze in strijd met het intellectuele-eigendomsrecht voor hen beschikbaar gestelde werken.

In *Glawischnig-Piesczek v Facebook Ireland* stelde het EHvJ vast dat een hosting provider gelast kan worden om berichten waarvan de inhoud eerder onwettig is verklaard te verwijderen of de toegang daartoe onmogelijk te maken, ongeacht wie om opslag van die informatie heeft verzocht. Dit betekent dat een internetplatform voor wat betreft die informatie en daarop gelijkende informatie verplicht kan worden tot filtering en blokkering (*notice and staydown*). Het gaat niet persé om identieke inhoud, maar wel om een dusdanige gelijkenis dat de hosting provider niet verplicht is tot een autonome beoordeling van de (on)rechtmatigheid.

Als wij deze uitspraken van het EHvJ toepassen in de context van horizontale privacyschendingen is er dus op grond van de Richtlijn elektronische handel geen algemene plicht voor tussenpersonen om pro-actief hun content te monitoren op mogelijk horizontale privacyschendingen, maar kunnen, afhankelijk van de omstandigheden van het geval tussenpersonen wel gedwongen worden om maatregelen te nemen om voor de toekomst inbreuken te voorkomen (*notice and staydown*).

Ook het EHRM heeft zich uitgesproken over de proportionaliteit van eventuele maatregelen die door tussenpersonen moeten worden genomen in *Delfi*. Voor de beoordeling of het proportioneel is om de tussenpersoon aansprakelijk te stellen en van deze maatregelen te verlangen weegt het Hof de volgende elementen:

1. De aard van de reacties (gaat het om ernstige inbreuken zoals bedreigingen of grove beledigingen).
2. De aansprakelijkheid van de auteurs (bestaan er realistische mogelijkheden om de auteurs te achterhalen en hen aansprakelijk te stellen).
3. De maatregelen die het platform heeft genomen (had het platform wetenschap kunnen/moeten hebben van de inbreukmakende gedragingen en welke reactieve en pro-actieve stappen had het platform moeten nemen).
4. De gevolgen voor het platform (wat is de impact van de aansprakelijkheid op het platform, maakt het bijvoorbeeld het bedrijfsmodel onmogelijk).

Met name element 3 is interessant omdat het Hof hier *in casu* overweegt dat wetgeving of jurisprudentie die pro-actieve stappen vereist van de tussenpersoon niet per se in strijd is met artikel 10 EVRM. Met andere woorden, de bescherming die tussenpersonen genieten onder artikel 14 van de Richtlijn Elektronische handel kan onder omstandigheden worden beperkt. Meer specifiek kan de *notice and takedown* regeling onvoldoende waarborgen bieden en moeten meer pro-actieve maatregelen worden genomen door het platform. Het Hof overweegt:

"the Court considers (…) that the rights and interests of others and of society as a whole may entitle Contracting States to impose liability on internet news portals, without contravening Article 10 of the

Convention, if they fail to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties."[254]

Voorts is interessant met het oog op het onderwerp van deze rapportage dat het Hof het feit dat de benadeelde niet op een effectieve manier de daadwerkelijke auteurs van de onrechtmatige uitingen kon aanspreken in rechte meeweegt. Het Hof overweegt:

"uncertain effectiveness of measures allowing the identity of the authors of the comments to be established, coupled with the lack of instruments put in place by the applicant company for the same purpose with a view to making it possible for a victim of hate speech to bring a claim effectively against the authors of the comments, are factors that support a finding that the Supreme Court based its judgment on relevant and sufficient grounds."[255]

Het vonnis werd destijds kritisch onthaald, omdat het het risico voor de gevolgen van onrechtmatige uitingen neerlegt bij de internettussenpersoon. Een mogelijk gevolg daarvan aldus critici, is dat dit zelfcensuur door de tussenpersoon in de hand werkt, hetgeen de vrijheid van meningsuiting en het recht op privacy aantast.[256]

In *MTE en Index.hu v. Hongarije* hanteerde de Grote Kamer van het Hof dezelfde toets, maar kwam tot een andere uitkomst.[257] *In casu* ging het om beledigende berichten die waren gepost op twee fora onder berichten over de praktijken van makelaarswebsites. Het Hof concludeert allereerst dat het oordeel van de nationale rechters dat een tussenpersoon die de mogelijkheid tot communicatie biedt moet verwachten dat daar misbruik van gemaakt kan worden en aldus de verantwoordelijkheid heeft om hierop toe te zien, in strijd met het EVRM is:

"82. The domestic courts held that, by allowing unfiltered comments, the applicants should have expected that some of those might be in breach of the law. For the Court, this amounts to requiring excessive and impracticable forethought capable of undermining freedom of the right to impart information on the Internet."

Het Hof overwoog voorts dat gezien de aard van de berichten een systeem van *notice and takedown* in dit geval voldoende was:

"91. However, in the case of Delfi AS, the Court found that if accompanied by effective procedures allowing for rapid response, the notice-and-take-down-system could function in many cases as an appropriate tool for balancing the rights and interests of all those involved. The Court sees no reason to hold that such a system could not have provided a viable avenue to protect the commercial reputation of the plaintiff. It is true that, in cases where third-party user comments take the form of hate speech and direct threats to the physical integrity of individuals, the rights and interests of others and of the society as a whole might entitle Contracting States to impose liability on Internet news portals if they failed to take measures to remove

[254] EHRM, 16 juni 2015, app. no. 64569/09 (*Delfi v. Estland*)
[255] EHRM, 16 juni 2015, app. no. 64569/09 (*Delfi v. Estland*)
[256] Zie bijvoorbeeld: https://edri.org/mte-v-hungary-the-ecthr-rules-again-on-intermediary-liability/
[257] EHRM, 2 februari 2016, app. no. 22947/13 (*Magyar Tartalomszolgáltatók Egyesülete & Index.hu ZRT v. Hongarije*)

clearly unlawful comments without delay, even without notice from the alleged victim or from third parties (see Delfi AS, cited above, § 159). However, the present case did not involve such utterances."

Het Hof nuanceert in deze uitspraak dus haar oordeel in *Delfi*, maar creëert hiermee tegelijkertijd een lastig probleem. Het Hof neemt in de weging of een partij pro-actieve maatregelen moet nemen de aard van de berichten als belangrijkste criterium: als het gaat om berichten die duidelijk illegaal of gevaarlijk zijn, dan kan van een tussenpersoon meer worden worden verwacht dan het enkel volgen van de *notice and takedown* regeling. Maar de vraag is hoe een provider op voorhand kan bepalen welke comments online komen en wat de aard daarvan is (enkel aanstootgevend of illegaal) zonder deze berichten vooraf te monitoren.

Als de aard van de *comments* de bepalende factor is dan doet een tussenpersoon er dus verstandig aan om pro-actief te gaan monitoren, omdat deze niet op voorhand kan vaststellen in welke gevallen berichtgeving tot aansprakelijkheid gaan leiden wegens het niet treffen van voldoende voorzorgsmaatregelen. Het risico dat door *Delfi* is ontstaan voor tussenpersonen is daarmee door dit vonnis dus niet noodzakelijkerwijs weggenomen.

10.2.3 Verstrekken van identificerende informatie van gebruikers

Naast het verwijderen, blokkeren of filteren van content kunnen internettussenpersonen ook helpen bij de bestrijding van horizontale privacyschendingen door identificerende gegevens van 'daders' door te geven aan de bevoegde autoriteiten en/of het slachtoffer.

Met betrekking tot het doorgeven van identificerende gegevens aan de bevoegde autoriteiten (de politie), geldt het regime voor het vorderen van identificerende gegevens (126na e.v. Sv). Voorwaarde is dat de horizontale privacyschending een strafbaar feit betreft (zoals bijvoorbeeld een bedreiging of de verspreiding van wraakporno).

Het doorgeven van identificerende gegevens aan het slachtoffer zodat deze weet wie de gewraakte uitspraken heeft gedaan en eventueel actie kan ondernemen, ligt een stuk gecompliceerder. Hoewel internettussenpersonen zelf kunnen beslissen of zij de identificerende gegevens van gebruikers verstrekken aan slachtoffers van horizontale privacyschendingen, doen zij dit in de regel niet. De reden hiervoor is dat zij dan in veel gevallen de AVG overtreden omdat het verstrekken van persoonsgegevens aan derden (anders dan aan bevoegde autoriteiten) doorgaans niet één van de verwerkingsdoelen is. De AVG biedt weliswaar de ruimte aan de verwerkingsverantwoordelijke om te beoordelen of een doorgifte toegestaan is, maar het risico voor een verkeerde beoordeling ligt bij de tussenpersoon.[258] De meeste providers zullen dit risico niet willen lopen en dus het niet verstrekken van de gegevens als uitgangspunt nemen. Dit betekent dat een slachtoffer zich tot de civiele rechter moet wenden om de tussenpersoon te dwingen om de identificerende gegevens te verstrekken.[259] Een dergelijke gang naar de rechter vormt

[258] De verwerkingsverantwoordelijke kan beoordelen of de verstrekking verenigbaar dan wel dat er een zelfstandige rechtsgrond ex. artikel 6 AVG is (bijvoorbeeld 6f AVG).
[259] Zie in dit kader: EHvJ, 21 januari 2008, nr. C-275/06 (*Promusicae v. Telefonica*), ECLI: ECLI:EU:C:2008:54 en EHvJ, 21 januari 2008, nr. C-461/10 (*Bonnier Audio*), ECLI: ECLI:EU:C:2012:219

waarschijnlijk voor veel betrokkenen een drempel, ook omdat op voorhand niet bekend is of de gegevens die de tussenpersoon heeft, daadwerkelijk de dader kunnen helpen identificeren.[260]

Wanneer een slachtoffer de civielrechtelijke weg bewandelt dan wordt in Nederland nog steeds de toets toegepast zoals deze is geformuleerd in het *Lycos/Pessers* arrest.[261] Een vordering tot het verstrekken van persoonsgegevens wordt alleen toegewezen wanneer:

a. de mogelijkheid dat de informatie, op zichzelf beschouwd, jegens de derde onrechtmatig en schadelijk is, voldoende aannemelijk is;
b. de derde een reëel belang heeft bij de verkrijging van de NAW-gegevens;
c. aannemelijk is dat er in het concrete geval geen minder ingrijpende mogelijkheid bestaat om de NAW-gegevens te achterhalen;
d. afweging van de betrokken belangen van de derde, de serviceprovider en de websitehouder (voor zover kenbaar) met zich meebrengt dat het belang van de derde behoort te prevaleren.[262]

Anders dan het vorderen van identificerende gegevens zijn er weinig (wettelijke) middelen om als benadeelde / slachtoffer actie te kunnen ondernemen. Na *Lycos Pessers* is er in de literatuur wel enige discussie geweest over de mogelijkheden voor benadeelden om eenvoudiger hun recht te halen. Zo stelde Ekker voor om de benadeelde (de eiser) in staat stellen om via de ISP een 'digitale dagvaarding' te laten sturen naar de verweerder.[263] Roosendaal heeft voorgesteld om naar Amerikaans en Canadees model een mogelijkheid te creëren om dagvaardingen te richten aan (op dat moment) anonieme internetgebruikers.[264] De ISP of een daartoe op te richten nationaal instituut kan de communicatie met de anonieme verweerder doen zonder diens anonimiteit direct op te heffen. Dit heeft voor de eiser het voordeel dat deze niet eerst de bekendmaking van de gebruikersgegevens via de rechter hoeft af te dwingen, voordat deze de echte rechtszaak kan starten. Een variant zonder directe rechtsgang is ook denkbaar. Een ISP of een onafhankelijk instituut kan bijvoorbeeld op verzoek van een benadeelde een notificatie sturen aan een gebruiker dat deze een onrechtmatige uiting heeft gedaan. Als de gebruiker niet reageert (bijvoorbeeld door excuses te maken of de onrechtmatige uitingen te verwijderen), dan worden de identificerende gegevens aan de benadeelde doorgegeven en kan deze zelf actie ondernemen. Hoewel deze voorstellen mogelijk een bijdrage kunnen leveren aan de bescherming van de horizontale privacy, zijn er tot op heden nog geen (grootschalige) initiatieven geweest om dit mogelijk te maken.

10.2.4 Strafrechtelijke aansprakelijkheid tussenpersonen

De strafrechtelijke aansprakelijkheid van tussenpersonen is in Nederland geregeld in artikel 54a Sr. Uitgangspunt is dat een internettussenpersoon alleen aansprakelijk is voor illegale content, wanneer deze geen gehoor geeft aan een bevel van de officier van justitie ex. artikel 125p Sv. Op grond van artikel 125p

[260] Zelfs bij platformen die een '*real name policy*' hanteren is er geen garantie dat de gebruikte accounts vals zijn.
[261] Zij bijvoorbeeld: Gerechtshof 's-Hertogenbosch, 11 juli 2018, 200.207.551_01, ECLI:NL:GHSHE:2018:2824
[262] Hoge Raad 25 november 2005, C04/234HR (*Lycos / Pessers*), ECLI:NL:HR:2005:AU4019
[263] Ekker. A. (2004), Annotatie bij Hof Amsterdam 24 juni 2004 (*Pessers/Lycos II*), in: *JAVI* 2004-5.
[264] Roosendaal, A. P. C. (2007). Elimination of anonymity in regard to liability for unlawful acts on the internet, in: *International Journal of Technology Transfer and Commercialisation*, 6(2/3/4), 184-195.

Sv kan de officier de aanbieder van een communicatiedienst in de zin van artikel 138g Sv (waar ook internettussenpersonen onder vallen) bevelen om bepaalde gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten. Hierbij moet het wel gaan om verdenking van een misdrijf als omschreven in artikel 67 eerste lid Sv. Dit laatste is vanuit het perspectief van horizontale privacyschendingen relevant, omdat dit delicten als belediging, smaad en laster uitsluit.

10.2.5 Rechtsvergelijking

Omdat met de Richtlijn Elektronische handel het aansprakelijkheidsregime voor internettussenpersonen geharmoniseerd is, zijn er op dit gebied weinig grote afwijkingen tussen de verschillende landen uit onze rechtsvergelijking. Wel zijn er lokale initiatieven en beleidsontwikkelingen die interessant zijn gericht op producenten en distributeurs en internettussenpersonen, deze worden hieronder besproken.

10.2.5.1 Duitsland

Duitsland kent een (beperkt) verbod op het voorhanden hebben van 'afluisterapparatuur' in artikel 90 van het *Telekommunikationsgesetz*. Volgens artikel 90 TKG is het verboden om zenders of andere telecommunicatieapparatuur die lijken op een ander voorwerp (bijvoorbeeld als ze daarin zijn verstopt of een ander voorwerp nabootsen) in eigendom te hebben, te vervaardigen of te distribueren. Het idee van de wetgever is dat dergelijke apparatuur in het bijzonder geschikt is om inbreuken te maken op de persoonlijke levenssfeer.[265]

Met betrekking tot de aansprakelijkheid van internettussenpersonen heeft Duitsland de Europese regels betreffende de aansprakelijkheid opgenomen in de *Telemediengesetz*.[266] Duitsland is echter een stap verder gegaan met betrekking tot de verantwoordelijkheid van internetplatformen via de Netwerkhandhavingswet (*Netzwerkdurchsetzungsgesetz,* NetzDG). Deze wet is gericht op internetdienstverleners die gebruikers in staat stellen informatie uit te wisselen en heeft tot doel om illegale content te bestrijden. Het gaat om informatie en gedragingen die strafbaar zijn gesteld in het Duitse wetboek van strafrecht. Naast zaken als het verspreiden van terroristische content en kinderpornografie zijn ook zaken als smaad en laster genoemd. Dit betekent dat ook 'eenvoudige' horizontale privacyschendingen binnen het bereik van de wet vallen.

De wet kent twee belangrijke verplichtingen voor internetplatformen: 1) zij moeten verantwoording afleggen over hun beleid met betrekking tot de verwijdering van illegale content en 2) zij zijn verplicht om een eenvoudig toegankelijk mechanisme voor het melden van illegale content te maken en moeten binnen 24 uur na de melding de betreffende content verwijderd hebben.

---

[265] Dierlamm, A., Cordes, M. (2018), '§ 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen', in: K.D. Scheurle & T. Mayen (red.) *Scheurle/Mayen Telekommunikationsgesetz Kommentar*, 2018, A., para 1. Zie voor een uitgebreide bespreking van het verbod: Galic, M. et. al. (2020), *Spioneren met hobbydrones en andere technologieën door burgers: een verkenning van de privacyrisico's en reguleringsmogelijkheden*, WODC

[266] *Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179)*

Er is scherpe kritiek geweest op de NetzDG, onder andere van de VN mensenrechtenrapporteur.[267] De voornaamste zorg is dat internetplatformen teveel censuur gaan toepassen op hun platform. Een studie van het CEPS stelt echter dat de wet vooralsnog niet heeft geleid tot een enorme toename in het aantal *takedown* verzoeken en ook niet heeft geleid tot een *'take down, ask later'* beleid bij de internetplatformen.[268] Of de wet het gewenste effect heeft gesorteerd is nog onduidelijk. Internetplatformen gebruiken primair hun *community standards* voor de verwijdering van illegale content en doen pas in tweede instantie een check of de content ook in strijd is met de NetzDG. Het daadwerkelijke effect van de wet lijkt daarmee eerder een snellere en meer consistente toepassing van de *community standards* te zijn. [269]

10.2.5.2 Polen

Polen heeft de Richtlijn elektronische handel geïmplementeerd in nationale wetgeving.[270] Een interessante ontwikkeling in Polen is dat de Poolse overheid afspraken gemaakt over het tegengaan van overblokkering met Facebook. Gebruikers kunnen bij een speciaal meldpunt terecht wanneer van mening zijn dat hun content onterecht verwijderd is. Facebook doet dan opnieuw een review op basis van hun community standards.[271]

10.2.5.3 Verenigd Koninkrijk

Naast de bescherming op grond van de Richtlijn elektronische handel hebben internetplatformen in het Verenigd Koninkrijk ook aanspraak op een vrijwaring van aansprakelijkheid op grond van de *Defamation Act 1996*. Wanneer de verweerder geen weet heeft of hoeft te hebben dat een uiting lasterlijk is, hij niet de auteur, redacteur of uitgever is en voldoende zorg heeft betracht, dan is deze niet aansprakelijk.

De Engelse regering publiceerde in 2019 een *White paper* over het tegengaan van *online harms*. Veel van de in dit paper besproken *harms* zijn te kwalificeren als horizontale privacyschendingen.[272] De Engelse regering is ook voornemens om de zorgplicht voor internettussenpersonen aan te scherpen. [273]

10.2.5.4 Zweden

In Zweden biedt de eerder genoemde BBS wetgeving de mogelijkheid om een houder van een berichtendienst aansprakelijk te stellen voor de verspreiding van illegale content. Hierbij is dus wel een voorwaarde dat de uiting op zichzelf strafbaar is.

---

[267] Zie: https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf
[268] Echikson, W., Knodt, O. (2018), *Germany's NetzDG: A key test for combatting online hate*, CEPS Research Report, no. 2018/09, November 2018, 1-2. Hierbij moet worden aangetekend dat de beschikbare cijfers een vertekend beeld laten zien omdat zij niet de door de platformen zelf verwijderde content meenemen, slechts de verwijdering op basis van een melding. Het kan zijn dat de NetzDG indirect heeft geleid tot een strengere interpretatie van de eigen community standards. Zie: Mouton, L. (2018), *Hate Speech op Facebook en Twitter: het verwijderen van berichten en accounts versus de vrijheid van meningsuiting*, Universiteit Gent, p. 110
[269] Tworek, H., Leerssen, P. (2019) *An Analysis of Germany's NetzDG Law, A working paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression*, p. 6.
[270] *Ustawa o świadczeniu usług drogą elektroniczną,* artikelen 12 tot en met 15
[271] 'Pierwsze tego typu porozumienie. Ministerstwo Cyfryzacji i Facebook - Ministerstwo Cyfryzacji - Portal Gov.pl' (*Ministerstwo Cyfryzacji*) <https://www.gov.pl/web/cyfryzacja/pierwsze-tego-typu-porozumienie-ministerstwo-cyfryzacji-i-facebook> Laatst geraadpleegd: 23 maart 2020.
[272] HM Government, *Online harms White Paper*, april 2019
[273] Ibid.

10.3 Politieke ontwikkelingen

Wat 'in redelijkheid te verlangen maatregelen' zijn om verschijning van privacyschendende of anderszins onrechtmatige uitingen te voorkomen, vormt momenteel het onderwerp van een brede internationale discussie. In Europees verband wordt al langere tijd gesproken over de aanpak van schadelijke illegale content.[274]

In september 2017 publiceerde de Europese Commissie een Mededeling over de bestrijding van illegale online content waarin zij nadrukkelijk wijst op de maatschappelijke verantwoordelijkheid van internetplatformen. Lidstaten worden opgeroepen om samen met de internetplatformen te komen tot effectieve manieren om schadelijke online content aan te pakken. In september 2018 werd deze Mededeling gevolgd door een *Aanbeveling voor een effectieve aanpak van illegale online content*.[275] Hierin worden concrete voorstellen gedaan zoals het stroomlijnen van meldingen, het aanstellen van *trusted flaggers* en het geautomatiseerd opsporen van illegale content. Om bovenmatige verwijdering te voorkomen moet er een systeem van hoor en wederhoor komen (tegenmeldingen). Hoewel de nadruk in beide beleidsstukken ligt op ernstige gedragingen zoals het aanzetten tot terrorisme, haatzaaien en de verspreiding van kinderpornografie, zijn zij voor de aanpak van (minder ernstige) horizontale privacyschendingen desalniettemin relevant, omdat veel van de mechanismen voor de aanpak van illegale content ook voor horizontale privacyschendingen werken.

In het bijzonder interessant is het voorstel voor de introductie van een *good samaritan clause*.[276] Internetplatformen zullen niet snel geneigd zijn om zich actiever met de inhoud te bemoeien met het oog op het bestrijden van horizontale privacyschendingen, omdat zij dan mogelijk hun aansprakelijkheidsvrijwaring kwijtraken. In de Verenigde Staten is om dit probleem op te lossen in de *Communications Decency Act* een zogenaamde *good samaritan clause* opgenomen. Deze clausule zorgt ervoor dat de aanprakelijkheidsvrijwaring voor internetplatformen intact blijft wanneer zij te goeder trouw zich pro-actief bemoeien met de content om schadelijke en illegale content te verwijderen. In het kader van de bestrijding van illegale content is een dergelijk voorstel ook in de Mededeling aangaande de bestrijding van illegale content gedaan.

De Europese Unie wil tenslotte het bestaande aansprakelijkheidsregime voor internettussenpersonen herijken. Hiertoe wordt de Richtlijn elektronische handel vervangen door een nieuwe *Digital Services Act*.[277] De verwachting is dat in deze nieuwe wetgeving een zorgplicht voor internetplatformen wordt opgenomen.[278]

[274] Zie bijvoorbeeld: Ullrich, C. (2017) *Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective*, JIPITEC
[275] Aanbeveling (EU) 2018/334 van de Commissie van 1 maart 2018 over maatregelen om illegale online-inhoud effectief te bestrijden
[276] Ibid.
[277] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf
[278] Zie in dit kader: https://www.politico.eu/wp-content/uploads/2019/08/clean_definite2.pdf

10.4 Afsluitende beschouwing

10.4.1 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 in Duitsland hebben wij een (beperkt) verbod op het gebruik van apparatuur die (ook) gebruikt kan worden om mensen af te luisteren gevonden. 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, dan wel het schenden van iemands privacy aanzienlijk eenvoudiger maken.

10.4.2 Aansprakelijkheid van internetussenpersonen

Internettussenpersonen spelen ongewenst een belangrijke rol bij horizontale privacyschendingen vanwege de communicatiemogelijkheden die zij bieden. Een deel van de oplossing voor de effectieve bestrijding van horizontale privacyschendingen ligt daarmee ook bij de internettussenpersonen, meer in het bijzonder de internetplatformen.

Met betrekking tot de rol van internetplatformen bij de bestrijding van horizontale privacyschendingen is de vraag in hoeverre zij aansprakelijk zijn voor het gedrag van gebruikers dan wel in hoeverre zij een plicht hebben om schendingen te voorkomen van belang. Op grond van de huidige Europese regeling (de Richtlijn elektronische handel), is het uitgangspunt dat internetplatformen 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 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 wel 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. 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 onrechtmatige uitingen, in het bijzonder wanneer dit op grote schaal en dus geautomatiseerd moet gebeuren. Dit kan ertoe leiden dat internetplatformen 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.

Mocht de wetgever overwegen een met Duitsland vergelijkbare regeling te introduceren in de Nederlandse rechtsorde, dan moet wederom rekening worden gehouden met de mogelijke effecten op de vrijheid van meningsuiting. De verwachting is dat wanneer platformen meer risico lopen op aansprakelijkheid, zeker als het een pro-actieve zorgplicht betreft, zij strenger zullen blokkeren en filteren om het risico van schadelijke of illegale content op hun platform te verkleinen. Deze zelfcensuur is een potentiële bedreiging voor de vrijheid van meningsuiting.[279] Ook kan het recht op privacy van gebruiker beïnvloeden omdat het platform meer toezicht op het eigen platform moet gaan houden.

10.4.3 Mogelijkheden voor individuen om hun rechten af te dwingen

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 op de internetplatformen en niet op de achterliggende gebruiker die daadwerkelijk de schending heeft gepleegd. Met name daar waar het gaat om het krijgen van schadevergoeding maakt dit de drempel

[279] Ullrich, C. (2017), Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective, in: *JIPITEC*, 8 (2017) 111 para 1.

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.

11 Overige mechanismen

Naast wettelijke normering en bescherming zijn er ook andere mechanismen die bijdragen aan het beschermen van de privacy in horizontale verhoudingen, het gaat dan primair om 1) zelfregulering en 2) onderwijs en voorlichting. Tenslotte kijken we ook kort naar regulering door de markt zelf.

11.1 Zelfregulering

Naast wet- en regelgeving van overheidswege zijn er ook zelfregulerende initiatieven om horizontale privacyschendingen tegen te gaan. Deze spelen zich op verschillende niveaus af en met uiteenlopende actoren.

11.1.1 Zelfregulering door burgers onderling

De voornaamste factor die het gedrag van burgers onderling reguleert daar waar het gaat om horizontale privacy, is de geldende maatschappelijke norm. Overtreding van deze normen worden geadresseerd door mechanismen als *naming and shaming*. Relevant is dat wat als maatschappelijk betamelijk of behoorlijk wordt gezien, mede door de digitalisering constant in flux is. Concrete zelfregulering op het gebied van privacy en gegevensbescherming is met name te vinden binnen beroepsgroepen (tuchtrecht) en in kleinere sociale verbanden zoals verenigingen. In de regels van sportverenigingen kunnen bijvoorbeeld regels opgenomen zijn over ontoelaatbaar gedrag zoals beledigingen.[280]

11.1.2 Zelfregulering door producenten en distributeurs

In ons onderzoek zijn wij geen zelfregulerende initiatieven tegengekomen van producenten en distributeurs van producten of diensten die in het bijzonder geschikt zijn om inbreuk te maken op de persoonlijke levenssfeer (zoals bijvoorbeeld *spycams* of *stalkerware*). Daar waar het gaat om de toepassing in de praktijk zien we wel initiatieven voor een zorgvuldige toepassing. Zo committeren particuliere recherchebureaus zich aan een Privacygedragscode die is goedgekeurd door de Autoriteit Persoonsgegevens.[281] Verder wordt via kenniscentra en brancheverenigingen zoals de Vereniging van Erkende Beveiligingsbedrijven, Het Centrum voor Criminaliteitspreventie en VNO-NCW / MKB Nederland geadviseerd over een zorgvuldige toepassing van bijvoorbeeld beveiligingscamera's. Het betreft hier echter wel primair de horizontale/diagonale verhouding bedrijfsleven-burger. Op het gebied van zorgvuldige toepassing van producten en diensten in de relatie burger-burger zijn er bij ons weten geen specifieke zelfregulerende initiatieven.

11.1.3 Zelfregulering door internettussenpersonen en -platformen

De internetplatformen hebben een bijzondere positie daar waar het gaat om de regulering van horizontale privacyschendingen. Via hun gebruiksvoorwaarden en *community standards* kunnen zij regels stellen aan het gebruik van hun diensten en deze ook daadwerkelijk handhaven. Zo kunnen de platforms content verwijderen die in strijd is met hun gebruiksvoorwaarden, kunnen zij gebruikers schorsen, en kunnen zij de

[280] Zie bijvoorbeeld: ECLI:NL:RBOVE:2017:4503
[281] https://autoriteitpersoonsgegevens.nl/nl/nieuws/besluit-privacygedragscode-sector-particuliere-onderzoeksbureaus-van-de-nederlandse

accounts van gebruikers volledig afsluiten.[282] De (grote) internetplatformen gebruiken veelal geautomatiseerde processen op basis van kunstmatige intelligentie om onrechtmatige content te herkennen en actie te ondernemen jegens gebruikers.

Naast strafbare gedragingen (zoals beelden van kindermisbruik of het aanzetten tot geweld) worden ook gedragingen die niet persé strafbaar zijn veelal niet toegestaan door internetplatformen omdat zij aanstootgevend kunnen zijn. Het gaat dan met name om naaktbeelden of beelden van geweld.[283]

Horizontale privacyschendingen zijn ook afgedekt in de community standaarden van diverse online dienstverleners, ook al zijn zij niet als 'horizontale privacyschendingen' geclassificeerd. Het gaat veeleer om het benoemen van concrete handelingen die niet toegestaan zijn zoals belediging, cyberpesten of het delen van naaktbeelden van derden.[284]

11.1.3.1 Zelfregulering op nationaal en internationaal niveau

Naast het reguleren van hun eigen online platformen zijn de internetplatformen ook actief in diverse nationale en internationale zelfregulerende initiatieven. Hieronder sommen wij de meest relevante initiatieven op.

The United Nations Guiding principles on business and human rights (de Ruggie principles)

Op mondiaal niveau bieden de United Nations Guiding principles on business and human rights (kortweg de *Ruggie principles*), een raamwerk voor bedrijven om hun bedrijfsvoering in lijn met mensenrechten uit te oefenen. De *Ruggie principles* beslaan het hele palet aan mensenrechten. Voor het onderwerp van dit onderzoek zijn de uitspraken van de Speciale Rapporteur van de Verenigde Naties voor de bevordering en bescherming van de vrijheid van meningsuiting in relatie tot de *Ruggie principles* van belang.[285] De Speciale Rapporteur heeft internetbedrijven opgeroepen om zich expliciet te committeren aan de *Ruggie Principles* en deze als uitgangspunt te nemen bij het opstellen van algemene voorwaarden en community standaarden en bij de beoordeling of content verwijderd moeten worden.[286]

Global Network Initiative

Het Global Network Initiative is een samenwerking van internetplatformen, telecompartijen en NGOs die gericht is op de vraag hoe technologiepartijen om moeten gaan met privacy en het recht op vrijheid van meningsuiting.[287] Het Global Network Initiative richt zich daarmee niet specifiek of exclusief op horizontale privacyschendingen, maar is wel een platform waar dit onderwerp op de agenda staat.

---

[282] Dit geldt naast sociale media platformen bijvoorbeeld ook voor aanbieders van app platformen zoals Google en Apple. Deze partijen kunnen op grond van hun geruiksvoorwaarden applicaties weren van hun platform, waardoor zij niet door gebruikers gebruikt kunnen worden.
[283] Zie bijvoorbeeld de *Facebook Community Standards*:
https://www.facebook.com/communitystandards/adult_nudity_sexual_activity
[284] Zie bijvoorbeeld: https://www.facebook.com/communitystandards of https://help.twitter.com/en/rules-and-policies#twitter-rules
[285] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations General Assembly, seventy fourth session, agenda item 70 (b) (A/74/486)
[286] Ibid.
[287] https://globalnetworkinitiative.org/

Christchurch Call
Naar aanleiding van de racistisch gemotiveerde massamoord in Christchurch hebben diverse internetplatformen en overheden gezamenlijk de *Christchurch Call* opgesteld.[288] In de *Christchurch Call* committeren overheden en internetplatformen zich tot acties om terroristische en extremistische content online te weren.

The EU Code of conduct on countering illegal hate speech online
Binnen de Europese Unie hebben diverse internetplatformen waaronder Facebook, Microsoft en Twitter zich verbonden aan de *EU Code of conduct on countering illegal hate speech online*. Via deze gedragscode committeren de internetplatformen zich aan het bestrijden van online haat.[289]

EU Alliance to better protect minors online
De Alliance to better protect minors online is een initiatief vanuit de Europese Unie waar diverse telecom en ICT partijen, NGOs en UNICEF in participeren. Het programma is gericht op het beschermen van kinderen tegen *harmful content*, *harmful conduct* (cyberpesten) en *harmful contact* (zoals *sextortion* en *grooming*).[290]

11.1.3.2 Nederlandse initiatieven
Binnen Nederland zijn er diverse zelfregulerende initiatieven in publiek-private samenwerking ontplooid die ook raakvlakken hebben met horizontale privacybescherming.[291] Allereerst is er de Nederlandse *Gedragscode notice and takedown* die het proces voor het doen van een melding (*notice*) tot en met het verwijderen of ontoegankelijk maken van de content (de *takedown*) beschrijft.[292] Daarnaast bestaat de *Gedragscode Abusebestrijding*.[293] Hoewel in deze gedragscode de nadruk ligt op cyberveiligheid vallen ook gedragingen die horizontale privacyschendingen opleveren binnen het bereik van de gedragscode.

11.2 Voorlichting, onderwijs en ondersteuning
In Nederland lopen diverse initiatieven om burgers 'mediawijs' en 'digitaal weerbaar' te maken. In Nederland is er met het programma Mediawijsheid een breed programma gericht op het voorlichten en onderwijzen van gebruikers op het gebied van verantwoord mediagebruik. Binnen het programma Mediawijsheid is ook aandacht voor de bescherming van horizontale privacy.[294] Zo zijn er dossiers over onder andere online omgangsvormen, *sexting*, online pesten, dreigtweets en haatberichten.[295] Naast Mediawijsheid zijn er campagnes en programma's zoals Alertonline.nl en Veiliginternetten.nl die meer gericht zijn op digitale veiligheid (*cybersecurity*) dan op horizontale privacyschendingen. Maar omdat veel digitale dreigingen (zoals *hacking* en *phishing*) direct of indirect ook tot een schending van de privacy leiden, zijn ze desalniettemin relevant.

[288] https://www.christchurchcall.com
[289] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en
[290] https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online
[291] Zie voor een overzicht: https://ecp.nl/
[292] https://noticeandtakedowncode.nl/ntd-code/
[293] https://www.abuseplatform.nl/gedragscode/
[294] https://www.mediawijsheid.nl/
[295] https://www.mediawijsheid.nl/dossiers

Naast specifieke voorlichtingsprogramma's zijn er ook stichtingen die zich richten op preventie en voorlichting. Denk bijvoorbeeld aan digitale burgerrechtenorganisaties zoals Bits of Freedom of organisaties zoals de Fraudehelpdesk.

Tenslotte zijn er organisaties die slachtoffers vertegenwoordigen of ondersteunen, bijvoorbeeld in collectieve procedures. In Nederland voeren de Stichting Stop Online Shaming en Helpwanted.nl rechtszaken namens slachtoffers van wraakporno, *sextortion* en andere vormen van *online shaming*.[296] De stichting Privacy First voert ook (collectieve) procedures vanuit een ideëel perspectief, maar deze zijn er vooralsnog primair op gericht om privacyschendingen door de overheid aan de kaak te stellen.

11.3 Regulering door de markt

Een laatste vorm van 'regulering' is spontane druk vanuit de markt, met name op bedrijven. Burgers en burgerorganisaties kunnen een moreel appèl doen op bedrijven om bij te dragen aan het beschermen van privacy. Op het moment dat burgers van mening zijn dat bedrijven online privacyschendingen faciliteren of zich daar onvoldoende van distantiëren, dan kunnen zij ook druk uitoefenen door middel van bijvoorbeeld boycots en *naming and shaming*. Maatschappelijke druk dwingt bedrijven dan om 'kleur te bekennen' en stelling te nemen tegen de maatschappelijke misstanden waarmee hun merken geassocieerd worden. Het effect daarvan is met name bij internetplatformen nu goed zichtbaar: adverteerders willen niet langer op bepaalde sociale media adverteren zolang deze partijen geen stappen ondernemen om mensenrechtenschendingen tegen te gaan.[297] Deze vorm van zelfregulering door de markt kan effectief zijn, omdat het direct de inkomsten van bedrijven raakt en hen daarmee dwingt om hun gedrag aan te passen. Wel is het de vraag of er sprake is van een blijvend effect en adverteerders bijvoorbeeld niet terugkomen op de platforms als de maatschappelijke onrust overgewaaid is.

11.4 Initiatieven in de onderzochte landen

In de door ons onderzochte landen zijn ook vanuit publieke en private hoek initiatieven op het gebied van voorlichting en onderwijs.

11.4.1 Duitsland

In Duitsland worden ouders en kinderen voorgelicht via Klicksafe.de.[298] Klicksafe maakt onderdeel uit van het EU brede *Better Internet for Kids* en *Safer Internet* Programma.[299]

11.4.2 Polen

In Polen worden kinderen en ouders ook voorgelicht over horizontale privacyschendingen via onder andere het Safer Internet programma. Programma's die specifiek gericht zijn op horizontale privacyschendingen zijn '*hug a hater*' (gericht op het kinderen bewust maken van *hate speech*) en *Think,*

[296] Zie: https://nos.nl/artikel/2324649-stiekem-gefilmde-beelden-online-pornosite-vagina-nl-voor-de-rechter.html
[297] Zie: https://www.theverge.com/21307454/unilever-verizon-coca-cola-starbucks-microsoft-ads-facebook
[298] https://www.klicksafe.de
[299] https://ec.europa.eu/digital-single-market/en/policies/better-internet-kids

don't send (gericht op het kinderen bewust maken van de gevaren van *sexting*). Voor ouders is er een programma gericht op *sharenting*.[300]

11.4.3 Verenigd Koninkrijk

In het Verenigd Koninkrijk zijn scholen verplicht om digitale vaardigheden en mediawijsheid te onderwijzen.[301] Het toezien op de ontwikkeling van deze digitale vaardigheden behoort tot de taken van telecomwaakhond Ofcom en zij doet ook veel onderzoek op dit gebied.[302] Ook voor volwassenen is er beleid voor de ontwikkeling van digitale weerbaarheid en vaardigheid.[303] Voor wraakporno bestaat er een specifieke hulplijn: *The Revenge Porn Helpline*.[304]

11.4.4 Zweden

Het Instituut voor Recht en Internet (*Institutet för juridik och internet*) is een NGO die zich richt op de bescherming van privacy online. De organisatie helpt slachtoffers van horizontale privacyschendingen met behulp van advies, maar ondersteunt hen ook bij rechtszaken.[305]

11.5 Afsluitende beschouwing

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

11.5.1 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 kan worden voor horizontale privacyschendingen (*spycams*, *stalkerware*) hebben wij niet kunnen vinden.

Zelfregulerende initiatieven om privacy in horizontale verhoudingen te beschermen spelen zich met name af 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 met name op het tegengaan van illegale content zoals beelden van kindermisbruik, racistische of xenofobische content (haatzaaien) en terroristische content (verheerlijken of aanzetten tot terrorisme).[306] 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*.

[300] Https://www.saferinternet.pl
[301] Zie: https://www.gov.uk/government/publications/education-for-a-connected-world
[302]https://www.ofcom.org.uk/research-and-data/media-literacy-research
[303]https://www.gov.uk/government/publications/essential-digital-skills-framework
[304]Zie bijvoorbeeld:https://revengepornhelpline.org.uk/other-support/
[305] http://www.juridikinstitutet.se/home-english/
[306] 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.

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:

"Despite taking steps to illuminate their rules and government interactions, the companies remain enigmatic regulators, establishing a kind of "platform law" in which clarity, consistency, accountability and remedy are elusive."[307]

11.5.2 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, met name de voorlichting gericht op kinderen, Europees gecoördineerd wordt. Hierdoor kunnen landen succesvolle campagnes en leertrajecten van elkaar overnemen.

[307] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations Human Rights Council, Thirty-eighth session, 18 June–6 July 2018, Agenda item 3, (A/HRC/38/35), p. 3

12 Overzicht wettelijke normering horizontale privacyschendingen

Op basis van de voorgaande hoofdstukken komen wij tot het volgende schematische overzicht van horizontale privacyschendingen en de normering en regulering daarvan.

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 handelspraktijken	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*.

13 Analyse en synthese

13.1 Horizontale privacyschendingen

Uit ons onderzoek blijkt dat privacyschendingen in horizontale verhoudingen op allerlei manieren plaatsvinden. Daarbij valt op dat uiteenlopende belangen en waarden in het geding zijn (veiligheid, eer en goede naam, vertrouwen in relaties *et cetera*) die allen bescherming genieten onder de noemer 'privacy'. De uiteenlopende waarden en belangen worden beschermd door een breed palet aan wet- en regelgeving.

Horizontale privacyschendingen worden mede mogelijk gemaakt door de snelle ontwikkeling van digitale technologieën. Daarbij gaat het enerzijds om producten en diensten die burgers en bedrijven in staat stellen om andere burgers te observeren en gegevens over hen vast te leggen (camera's, *smartphones*, *drones*, *Internet of Things* toepassingen, *spyware*) en anderzijds om diensten en platformen (*instant messaging*, *social media*, discussiefora) die burgers in staat stellen om op grote en minder grote schaal gegevens met elkaar te delen.

De digitale informatiecultuur die voortvloeit uit deze ontwikkelingen is nog volop in ontwikkeling en verandert continu. Datzelfde geldt tot op zekere hoogte voor de bijbehorende normen en waarden, omgangsvormen en privacyverwachtingen. Daar waar er in de fysieke wereld duidelijke omgangsvormen zijn en een min of meer gedeeld beeld bestaat van wat een redelijke privacyverwachting is, is dit beeld met name in de online wereld meer diffuus. Dat heeft mede tot gevolg dat privacyschendingen sneller en frequenter plaatsvinden.

13.2 Horizontale werking van het recht op privacy

De horizontale werking van grondrechten wordt erkend binnen alle landen die zijn betrokken in de rechtsvergelijking. Enerzijds via de jurisprudentie van het EHRM, anderzijds via nationale jurisprudentie en/of grondwettelijke bepalingen.

De werking van grondrechten in horizontale relaties wordt in de door ons onderzochte landen op uiteenlopende wijze geconstrueerd. In Polen wordt bijvoorbeeld de horizontale werking van grondrechten expliciet in de grondwet onderkend, terwijl in Duitsland deze wordt afgeleid uit de grondwettelijk beschermde menselijke waardigheid. In Nederland is de horizontale werking van grondrechten door de Hoge Raad afgeleid van het algemene persoonlijkheidsrecht dat op haar beurt voortvloeit uit de menselijke waardigheid. Omdat de menselijke waardigheid geen zelfstandige bescherming kent in Nederlandse Grondwet, heeft de Hoge Raad dus als het ware *extra legem, intra ius* de horizontale werking van grondrechten geconstrueerd.

Hoewel in de rechtstradities van de onderzochte landen de onderkenning van de horizontale werking van grondrechten op verschillende wijzen tot stand is gekomen, zien wij niet direct grote verschillen in de mate van bescherming. In Zweden is de erkenning van de horizontale werking van grondrechten vanuit de

nationale rechtsorde het minst sterk, maar ook daar is via de werking van het EVRM de horizontale werking van grondrechten geaccepteerd.

Het verstevigen van de juridische basis van de horizontale werking van het recht op privacy, naar bijvoorbeeld Pools of Duits model, lijkt daarom naar het oordeel van de onderzoekers niet noodzakelijk. Van tijd tot tijd wordt ook geopperd om naar analogie van het in de Duitse rechtspraak ontwikkelde concept van de 'informationele zelfbeschikking', de grondwettelijke bescherming van het recht op gegevensbescherming uit te breiden. Voor het antwoord op de vraag of dit verstandig is refereren wij graag aan het oordeel van de Commissie Franken uit 2000. Een recht op informationele zelfbeschikking zou met het oog op de beschermen van de rechten en vrijheden van anderen sterk geclausuleerd moeten zijn. Een dergelijk 'veel geven en vervolgens weer veel terugnemen' voegt daarmee weinig toe aan de rechtsbescherming van burgers. Voorts moet geconcludeerd worden dat de zelfstandige gelding van een recht op informationele zelfbeschikking met het oog op de Nederlandse gebondenheid aan het Europees recht (meer in het bijzonder de AVG) überhaupt beperkt zal zijn. Ook lijkt het geven van meer controle aan burgers om hun eigen privacy te beschermen een schijnoplossing die de *status quo* en normalisering van privacyinbreuken in de hand kan werken. Burgers zijn momenteel niet geëquipeerd om tegen alle mogelijke privacyinbreuken op te komen en zelf hun rechten juridisch af te dwingen.

Tenslotte rijst de vraag in hoeverre een grondwettelijke verankering van de horizontale werking van grondrechten bijdraagt aan de rechtsbescherming in materiële zin als er niet tegelijkertijd mogelijkheden worden gecreëerd om deze rechten ook af te dwingen via een effectieve rechtsgang.

Wij concluderen daarom dat gegeven de indirecte horizontale werking van grondrechten via het EVRM en het bestaan van een algemeen persoonlijkheidsrecht in Nederland, de horizontale werking van het recht op privacy op 'grondrechtelijk niveau' afdoende geborgd is.

Vanuit grondrechtelijk perspectief is het bij de normering en bescherming van privacy in horizontale verhouding van belang in het oog te houden dat het recht op privacy en de vrijheid van meningsuiting 'communicerende vaten' zijn. Versterking van het recht op privacy, bijvoorbeeld door verdergaande strafbaarstellingen van inbreuken op de horizontale privacy, kunnen hun weerslag hebben op de vrijheid van meningsuiting. Bij de botsing van het recht op vrijheid van meningsuiting en het recht op privacy moet de clausulering van artikel 10 lid 2 EVRM richtinggevend blijven.

13.3 Normering en bescherming tegen horizontale privacyschendingen in Nederland

De normering en bescherming van het recht op privacy in horizontale verhoudingen krijgt daadwerkelijk gestalte in lagere wetgeving zoals het strafrecht, het gegevensbeschermingsrecht, administratief recht en het civiel recht.

13.3.1 Strafrecht

Het Wetboek van Strafrecht stelt veel schendingen van privacy in horizontale verhoudingen strafbaar. De strafrechtelijk beschermde belangen die in het geding zijn bij schendingen van de horizontale privacy zijn bovenal: de menselijke waardigheid (de eer en de goede naam in het bijzonder), de lichamelijke en geestelijke integriteit van een persoon en de goede zeden.

Bij de strafbaarstelling zien we dat enerzijds algemene delicten (bedreiging, belediging, belaging) ook in de context van (digitale) schendingen van de privacy in horizontale verhoudingen goed kunnen worden toegepast en anderzijds dat er delictsomschrijvingen zijn die specifiek gericht zijn op het sanctioneren van bepaalde digitale privacyschendingen (wraakporno, heimelijk cameratoezicht).

De Nederlandse catalogus van delictsomschrijvingen wijkt op hoofdlijnen niet af van die in de door ons onderzochte landen. De belangrijkste verschillen zijn dat er 1) in Polen en het Verenigd Koninkrijk bredere strafbaarstellingen zijn voor het verspreiden of toezenden van aanstootgevende content en 2) dat er in Duitsland en Zweden uitgebreide strafbaarstellingen zijn voor het filmen van hulpbehoevenden.

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 is. Dit heeft mogelijk niet alleen een effect op vrije informatiegaring en verspreiding door het individu, maar ook op de (professionele) journalistiek en media.

Een strafrechtelijke bepaling die in aanmerking kan komen voor 'transplantatie' in de Nederlandse strafwet is het filmen van hulpbehoevende personen. Mogelijke negatieve effecten van een dergelijke strafbaarstelling zijn dat beelden van omstanders bij bijvoorbeeld misdrijven of verkeersongelukken die kunnen bijdragen aan de opheldering van het misdrijf of de toedracht van een ongeluk niet meer worden gemaakt. Verder kunnen de beelden ook relevant zijn bij aansprakelijkheids- en verzekeringskwesties. Bij een eventuele strafbaarstelling moet met deze effecten rekening worden gehouden.

Bij de strafrechtelijke normering moet wel in ogenschouw worden genomen dat het strafrecht *ultimum remedium* is. Wanneer er bijvoorbeeld op grond van het civiel recht of het gegevensbeschermingsrecht ook mogelijkheden zijn om op te treden tegen privacyschendingen, dan verdient dat de voorkeur. De vraag is daarmee in hoeverre een grotere nadruk op strafrechtelijke regulering van horizontale privacy wenselijk is. In horizontale verhoudingen gaat het bij veruit de meeste privacyinbreuken om relatief kleine schendingen met beperkte gevolgen; het strafrecht lijkt dan een minder voor de hand liggend middel om op te treden tegen dit soort alledaagse inbreuken.

13.3.2 Gegevensbeschermingsrecht

Het gegevensbeschermingsrecht is primair op EU niveau gereguleerd, door middel van de Algemene Verordening Gegevensbescherming. Daarin staan allerhande rechten, plichten en voorwaarden voor een legitieme gegevensverwerking. Deze Verordening is ook van toepassing in horizontale verhoudingen,

zolang er geen sprake is van een verwerking voor puur persoonlijke doeleinden. Is de 'huishoudexceptie' niet van toepassing, dan moeten burgers die gegevens over anderen verzamelen een legitiem doel dienen hebben voor de verwerking, ook moeten zij voldoen aan de overige vereisten uit de AVG.

Het ligt niet voor de hand dat Nederland nadere gegevensbeschermingsregels stelt voor horizontale verhoudingen. De AVG laat daar weinig ruimte toe; bovendien is het probleem niet dat er lacunes zijn in de materiële rechtsregels. Veeleer gaat het om de vraag hoe voor de naleving van de regels dient te worden gezorgd. Burgers zijn vaak niet op de hoogte van het feit dat er gegevens over hen worden verzameld, door *smartphones*, beveiligingscamera's, spionageproducten, *drones* of andere apparatuur. Bovendien zijn dergelijke producten zo wijdverbreid, en is de verwachting dat deze in de toekomst alleen maar een grotere rol zullen spelen in de samenleving, dat het voor burgers vrijwel ondoenlijk is om bij alle mogelijke verwerkingen na te gaan wie de verwerkingsverantwoordelijke is, of aan alle regels van de AVG is voldaan en zo niet, om een rechtszaak te beginnen. Daarnaast zijn burgers vaak zelf niet op de hoogte dat wat zij doen met die techniek onder de AVG valt en dat ze zich zouden moeten inhouden met het verwerken van gegevens over anderen.

Een oplossing hiervoor is niet eenvoudig te vinden. Nederland zou kunnen overwegen om meer rechtsmiddelen te geven aan burgerrechtenorganisaties die in rechte opkomen voor de privacybelangen van burgers (zoals bijvoorbeeld het Instituut voor Internet en Recht in Zweden doet), maar dit zal zich nog steeds richten op de meer in het oog springende privacyschendingen met grotere gevolgen en niet op kleine en alledaagse incidenten, zoals een *drone* die in de tuin van de buurman opnames maakt. Dat geldt ook voor de handhaving van het gegevensbeschermingsrecht door de Autoriteit Persoonsgegevens. Het zou onevenredig veel middelen en mankracht kosten voor de AP om allerhande kleine privacyinbreuken te controleren en te bestraffen.

13.3.3 Administratief recht, mededingingsrecht en consumentenbescherming

Het algemeen administratief recht is als zodanig van beperkt belang in horizontale verhoudingen. Wel kan het een rol spelen bij de handhaving en naleving van bepaalde normen. Een voorbeeld daarvan is dat veel Algemene Plaatselijke Verordeningen regels stellen die zien op de bescherming van onderlinge privacy. Zo bepaalt de APV van Amsterdam: "*Het is verboden bewakingsapparatuur te gebruiken wanneer daarmee personen kunnen worden waargenomen in een ander gebouw, vaartuig of besloten erf dan waar de bewakingsapparatuur staat opgesteld. Het is verboden zich op of aan de weg op te houden met de kennelijke bedoeling personen die zich op of aan de weg of in een gebouw of vaartuig bevinden te bespieden.*"[308] Daarnaast verbiedt de APV ook geluidsoverlast en hinderlijk gedrag. Daarvan kan bijvoorbeeld sprake zijn bij het geval van drones die geluidshinder veroorzaken en over de heg in de achtertuin van de buren kunnen vliegen.

Het mededingingsrecht en het consumentenrecht kunnen nuttige aanvullingen bieden voor de bescherming van horizontale privacy, primair in diagonale verhoudingen, dat wil zeggen burger-(internet)bedrijf. De European Data Protection Supervisor heeft er op gewezen dat de interactie tussen het

[308] Verordening van de gemeenteraad van de gemeente Amsterdam gemeentelijke regelgeving op het gebied van openbare orde en veiligheid Algemene Plaatselijke Verordening 2008

consumentenrecht, het mededingingsrecht en het gegevensbeschermingsrecht essentieel is voor een goede regulering van de *Big Data* samenleving.[309]

Het consumentenrecht verbiedt onder meer het aanbieden van producten en diensten als zijnde gratis, terwijl ze dat niet zijn. Het is de vraag of het aanbieden van internetdiensten, waarbij de burger 'betaalt' met zijn persoonsgegevens, onder zo'n verbod zou vallen. Ook is het de vraag of de contractuele bepalingen die burgers moeten ondertekenen wel rechtsgeldig zijn en of de ondertekende contracten nietig dan wel vernietigbaar zouden kunnen zijn vanwege een gebrekkig tot stand gekomen wil, een gebrek aan relevante informatie of dwaling aan de zijde van de burger. Uit onze rechtsvergelijking blijkt dat de bestudeerde landen op dit punt niet wezenlijk meer duiding bieden. Nederland zou het voortouw kunnen nemen door meer specifiek aan te geven hoe het consumenten- en contractenrecht specifiek moet worden begrepen in de digitale omgeving.

Dat geldt ook voor het mededingingsrecht. Zowel op Europees niveau als op landelijk niveau, zoals bijvoorbeeld Duitsland, is het mededingingsrecht reeds met succes ingezet om machtsconcentraties, koppelverkoop en machtsmisbruik door grote internetbedrijven als Google, Facebook en Microsoft tegen te gaan. In Nederland zou de Autoriteit Consument en Markt een speerpunt kunnen maken van de digitale omgeving om zodoende de privacy in diagonale verhoudingen (en daarmee indirect in horizontale verhoudingen) beter te beschermen.

13.3.4 Civiel recht

Het civiel recht biedt via de actie uit onrechtmatige daad voldoende mogelijkheden om op treden tegen horizontale privacyschendingen. Naast rectificatie of verwijdering kan zowel materiële als immateriële schade worden vergoed. Bij dat laatste is het wel moeilijk om de schade van een privacyschending te kwantificeren.

Gezien het feit dat vaak niet te voorspellen wanneer een privacyschending plaats gaat vinden en wie daarvoor verantwoordelijk is, is het moeilijk om pro-actief op te treden en schendingen te voorkomen. In tegenstelling tot het klassieke medialandschap waar door het verbieden van onrechtmatige publicaties (grotere) schade aan de privacy voorkomen kan worden, is er geen preventieve actie in de online wereld waar iedereen met een druk op de knop een uiting kan doen. De enige mogelijkheid die dan rest is het doen van *damage control* via *takedown* verzoeken. Door het gemak waarmee content viraal gaat is dit echter een moeizaam proces omdat alle partijen die de content plaatsen individueel moeten worden aangesproken.

13.4 De rol van producenten, distributeurs en internettussenpersonen

Technologische ontwikkelingen op het gebied van hardware (camera's, *drones, dashcams, Internet of Things*) en software (gezichtsherkenning, *stalkerware*) maken horizontale privacyschendingen steeds eenvoudiger en potentieel ingrijpender. Toch zijn er -met uitzondering van Duitsland- geen strenge(re) regels voor de productie en verkoop van hardware en software die geschikt zijn voor het maken van

[309] European Data Protection Supervisor (2016), *Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data*

inbreuken op de privacy. Dit valt te verklaren vanuit het feit dat zelfs apparatuur die hoofdzakelijk of exclusief gebruikt wordt voor het bespioneren van mensen (*spycams*, *stalkerware*) onder omstandigheden legitiem kan worden toegepast. Het betreft dan overigens wel voornamelijk toepassingen in de relatie burger-bedrijfsleven, zoals de toepassing van heimelijk cameratoezicht om diefstal op te sporen. Naast afwezigheid van *ex ante* beperkingen aan de productie en verkoop van hardware en software die in het bijzonder geschikt is om privacyinbreuken te maken zien we ook geen zelf-regulerende initiatieven vanuit fabrikanten of distributeurs om privacyschendingen tegen te gaan.

In de online wereld zien we wel zelfregulering gericht op het tegengaan van horizontale privacyschendingen. Het zijn met name de internetplatformen zelf die op grond van hun gebruiksvoorwaarden handhavend optreden. Hoewel zelfregulering via gebruiksvoorwaarden een krachtig instrument is om horizontale privacyschendingen tegen te gaan, zijn er ook zorgen over mogelijke ongewenste neveneffecten. De Speciale VN Rapporteur voor de vrijheid van meningsuiting is kritisch over de vrijblijvendheid, gebrek aan transparantie en willekeur waarmee internetplatformen kunnen handhaven.[310]

Daar waar het gaat om handhaving hebben internetplatformen op grond van de Richtlijn elektronische handel momenteel géén plicht om pro-actief hun platformen te monitoren op schadelijke of illegale content. Wel bestaat de wens om internetplatformen meer verantwoordelijkheid te geven (een zorgplicht) bij het tegengaan van schadelijke en illegale content. In haar *political guidelines* zet de voorzitter van de Europese Commissie uiteen dat zij voornemens is om de regels op het gebied van de aansprakelijkheid van internetplatformen te herzien.[311]

De Speciale VN rapporteur is echter in zijn meest recente rapport ook kritisch over de wens van staten om de platformen te verplichten om bijvoorbeeld upload filters te installeren:

"The push for upload filters for hate speech (and other kinds of content) is ill-advised, as it drives the platforms towards the regulation and removal of lawful content. They enhance the power of the companies with very little, if any, oversight or opportunity for redress."[312]

Vooralsnog zijn er in de door ons onderzochte landen geen uploadfilters geïntroduceerd. De Duitse *Netzwerkdurchsetzungsgesetz* kent de meest verstrekkende verplichtingen voor internetplatformen daar waar het gaat om het actie ondernemen tegen illegale content. De belangrijkste kritiek op de Duitse wet is dat deze tot (zelf)censuur leidt.

Hoewel er voor de specifieke situatie in Duitsland (nog) geen bewijs is dat strengere regelgeving leidt tot (zelf)censuur bestaat dat risico wel. Niet alleen de platformen zouden zichzelf kunnen gaan censureren, ook de gebruikers zelf kunnen dit doen. Onderzoek naar het gedrag van gebruikers die zich met een *takedown*

[310] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations Human Rights Council, Thirty-eighth session 18 June–6 July 2018, Agenda item 3, (A/HRC/38/35), p. 3
[311] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.
[312] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations General Assembly, seventy fourth session, agenda item 70 (b) (A/74/486), p. 15

verzoek geconfronteerd zagen laat zien dat deze gebruikers in de toekomst terughoudender omgingen met het posten van content online.[313] Tegelijktertijd kan dit ook als een positief effect worden gezien, omdat dit blijkbaar, in tegenstelling tot het enkel hebben van wet- en regelgeving, wel leidt tot normoverdracht.

13.5 Effectiviteit van de rechtsbescherming

Hoewel een toets van de effectiviteit van privacybeschermende maatregelen niet de primaire opdracht voor dit onderzoek vormde en wij aldus niet empirisch hebben getoetst of de door het recht geboden privacybescherming daadwerkelijk in de praktijk wordt gerealiseerd, kunnen daar op basis van ons onderzoek in ieder geval wel vraagtekens bij worden geplaatst.

Al wordt de horizontale werking van grondrechten erkend, het primaire uitgangspunt blijft dat in horizontale relaties partijen min of meer gelijkwaardig zijn en aldus onderling eventuele geschillen moeten oplossen. Dit veronderstelt dat er voor deze partijen een effectieve rechtsgang is. Nu is deze er wel (bijvoorbeeld de gang naar de civiele rechter), maar de eigenschappen van het internet maken deze rechtsgang wel moeilijker. Veel horizontale privacyschendingen, zeker daar waar het gaat om het doen van uitingen en het openbaarmaken en verspreiden van privé-informatie, vinden anoniem of pseudoniem plaats. Een slachtoffer kan in dat geval meestal niet direct zelf actie ondernemen tegen de dader, maar moet zich wenden tot de internettussenpersoon.[314] Er komt daarmee een verantwoordelijkheid te rusten op de schouders van deze tussenpersonen die, afgezien van het voorkomen van aansprakelijkheid en reputatieschade, niet direct een belang hebben bij het vervullen van een dergelijke bemiddelingsfunctie.

Naast de burger zelf speelt de overheid een rol bij het beschermen van de horizontale privacy. De overheid heeft een positieve verplichting om de rechten van burgers effectief te beschermen. De overheid vervult deze taak door de normering van horizontale privacyschendingen en de handhaving via onder andere het strafrecht, het gegevensbeschermingsrecht, het administratieve recht en andere rechtsgebieden zoals in dit rapport beschreven.

In de horizontale relatie burger-bedrijfsleven speelt het gegevensbeschermingsrecht (de AVG) de belangrijkste rol. Maar daar waar het gaat om schendingen van de horizontale privacy in de relatie burger-burger is het gegevensbeschermingsrecht in de praktijk nagenoeg onzichtbaar. Dit valt deels te verklaren vanuit de materiële reikwijdte die verwerking voor zuiver huishoudelijke doelen uitsluit, maar zeker ook door de prioriteitstelling en capaciteit van de toezichthouder om in te grijpen. De toezichthouder geeft zelf regelmatig aan onvoldoende capaciteit te hebben waardoor voor de aanpak van horizontale schendingen van de privacy door burgers onderling waarschijnlijk weinig ruimte bestaat.[315]

Met de bovenstaande beschouwing in het achterhoofd, is het de vraag of de onderverdeling horizontaal/verticaal überhaupt wel een relevant denkkader biedt. Het standpunt dat partijen in horizontale

[313] Penney, J. (2020), Privacy and Legal Automation: The DMCA as a Case Study, in: Stanford Technology Law Review, Vol. 22, No. 1, 412
[314] Dit probleem wordt nog groter op het moment dat de verweerder onbekend is, bijvoorbeeld omdat diens identificerende gegevens onbekend zijn.
[315] Zie bijvoorbeeld: https://autoriteitpersoonsgegevens.nl/nl/nieuws/forse-stijging-privacyklachten-2019

verhoudingen min of meer gelijkwaardig zijn is zeker in de relatie burger-bedrijfsleven niet houdbaar. Veel (grote) bedrijven hebben een duidelijk sterkere machtspositie ten opzichte van de burger (vandaar dat wij spreken van diagonale verhoudingen). Via mechanismen als het consumentenrecht en het gegevensbeschermingsrecht wordt de ongelijke horizontale verhoudingen tussen bedrijven en burgers deels gerepareerd. Vanuit het perspectief van rechtsbescherming is er dus eigenlijk ook geen sprake meer van een zuivere horizontale verhouding in de relatie burger-bedrijfsleven. Een ander aspect dat de verhoudingen verder vertroebelt is samenwerkingen tussen de overheid en private partijen (publiek-private samenwerking). Binnen dergelijke samenwerkingen worden gegevens uitgewisseld en kan er sprake zijn van een significante inmenging in de persoonlijke levenssfeer van de burger. Belangrijker dan het onderscheid horizontaal / verticaal is daarom zorgen voor een rechtsbescherming die past bij de verhoudingen tussen partijen.

13.6 Toekomstige regulering van horizontale privacyschendingen

Met betrekking tot de normering en regulering van het recht op privacy in horizontale verhoudingen onderscheiden wij drie niveaus:

1) Het grondwettelijke niveau
2) Het niveau van de formele wet- en regelgeving (strafrecht, civiel recht, *et cetera*), en
3) De uitvoer en handhaving van de wet- en regelgeving.

Dit onderscheid biedt een denkkader voor de toekomstige regulering van horizontale privacyschendingen.

Het beeld dat uit ons onderzoek naar voren komt is dat het eerste niveau de (grondwettelijke) bescherming van privacy in horizontale verhoudingen, afdoende geborgd is binnen Nederland. Op het niveau van de grondwettelijke bescherming wijkt Nederland in ieder geval niet noemenswaardig af van de door ons onderzochte landen. Dit valt waarschijnlijk te verklaren vanuit het feit dat alle landen betrokken bij de rechtsvergelijking uit een gedeelde Europese (juridische) traditie komen en via het EVRM de grondwettelijke bescherming min of meer geharmoniseerd is.

Op het tweede niveau, dat van de formele wetgeving, zien we in onze rechtsvergelijking ook relatief weinig verschillen tussen de landen. Er zijn dan ook eigenlijk geen rechtsfiguren waarvan de transplantatie in Nederland direct noodzakelijk is, bijvoorbeeld om een gat in de rechtsbescherming op te vullen. Wel kunnen bepaalde rechtsfiguren ter inspiratie dienen voor een verdere versterking van het recht op privacy in horizontale verhoudingen. Denk aan een verbod op afluisterapparatuur, of de strafbaarstelling van het filmen van hulpbehoevenden.

De inrichting van niveau twee heeft zijn weerslag op niveau drie: de daadwerkelijke uitvoer en handhaving.

Als het aankomt op de inrichting van juridische maatregelen op het tweede niveau zijn er grofweg twee opties: 1) maatregelen nemen die zijn gericht 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. Het grootste voordeel van deze aanpak is dat schendingen voorkomen kunnen worden. 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 onmogelijk wordt gemaakt door een verbodsbepaling. Het nadeel van *ex post* regulering 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 alvorens 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, er bewijsrechtelijke obstakels bestaan, de schade vaak 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 het richten van maatregelen niet zozeer op 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. In Duitsland is er sprake van strengere wetgeving voor internettussenpersonen. Verder is er momenteel op Europees niveau een brede discussie over de verantwoordelijkheid van Internettussenpersonen in het kader van de *Digital Services Act*.

Bij horizontale privacyschendingen bestaat er altijd het spanningsveld tussen het recht op de bescherming van de privacy enerzijds en het recht op andere rechten (in het bijzonder het recht op vrijheid van meningsuiting) anderzijds. Structurele maatregelen die gericht zijn op het terugdringen van horizontale privacyschendingen hebben onherroepelijk een effect op de vrijheid van meningsuiting. Zo zal de mogelijkheid om niet anoniem/pseudoniem te posten op sociale media wellicht bijdragen aan het terugdringen van horizontale privacyschendingen omdat daders zich niet langer onkwetsbaar wanen, maar een dergelijke maatregel kan ook verstrekkende gevolgen hebben voor de vrijheid van meningsuiting. Ook het blokkeren en filteren van content kan grote gevolgen hebben voor de vrijheid van meningsuiting, niet in de laatste plaats omdat in tegenstelling tot bijvoorbeeld auteursrechtelijk beschermde werken privacyschendingen veel meer contextgebonden zijn. Het risico op vals-positieven en vals-negatieven is daarmee aanzienlijk.

Nederland werkt momenteel primair met vormen van *ex post* regulering, kent een algemene zorgplicht en werkt slechts in zeer beperkte mate met *ex ante* regulering. Uit de rechtsvergelijking en het literatuuronderzoek komt eenzelfde soort beeld naar voren voor de onderzochte landen. Ook zij zetten

primair in op *ex post* regulering. Uit onze studie blijkt dat de catalogus van normstellende bepalingen in het strafrecht, gegevensbeschermingsrecht en civiel recht in Nederland niet wezenlijk verschilt van andere landen.

Wanneer wij kijken naar het derde niveau, dan is het de vraag of de (grond)wettelijke bescherming die de burger geniet ook daadwerkelijk in de praktijk afgedwongen kan worden. Onze inschatting is dat dit momenteel niet of onvoldoende het geval is. Burgers kunnen zich steeds moeilijker onttrekken aan privacyschendingen als gevolg van de ruime beschikbaarheid van opnameapparatuur (*smartphones*, *Internet of Things*, *drones*, spycams *et cetera*) en de mogelijkheden die het internet en de sociale media bieden voor het verspreiden van beelden en andere privé-informatie. Onze voorzichtige conclusie is dat zonder innovaties in het procesrecht (bijvoorbeeld *ex parte* procedures voor ernstige privacyschendingen), de mogelijkheden tot het uitoefenen van het recht op privacy in horizontale verhoudingen ontoereikend zijn. Voor wat betreft de handhaving via het strafrecht en het gegevensbeschermingsrecht is ons idee dat de capaciteit tekortschiet voor een effectieve handhaving. Het verbeteren van de mogelijkheden voor burgers om hun rechten af te dwingen en het verbeteren van de handhaving lijken daarmee de meest kansrijke opties om de horizontale privacy beter te beschermen.[316]

Ook hieruit volgt echter een spanningsveld. Enerzijds is er een behoefte om burgers meer mogelijkheden te geven om effectief op te treden tegen schendingen van hun privacy. Anderzijds moet gewaakt worden tegen het ontstaan van een claimcultuur. Dit spanningsveld bestaat ook bij handhaving door de overheid. Het Openbaar Ministerie en de Autoriteit Persoonsgegevens, richten zich nu met name op de ernstige en ingrijpende privacyschendingen in horizontale relaties, zoals bijvoorbeeld het heimelijk maken en verspreiden van videobeelden in sauna's of kleedruimtes. Waar met name winst te behalen is, is in het aanpakken van de kleinere privacyschendingen, die ieder afzonderlijk van elkaar geen grote schade toebrengen, maar bij elkaar genomen wel. Maar overheidsdiensten meer macht en middelen geven om alledaags gebruik van technologie en applicaties te controleren kan leiden tot een *Big Brother* overheid die burgers in hun alledaagse bezigheden nauwgezet controleert. Het gevaar is dan dat de remedie erger wordt dan de kwaal.

Omdat horizontale privacy zo'n breed scala aan waarden en belangen beslaat, is het verstandig om nauwkeurig te monitoren welke nieuwe vormen van horizontale privacyschendingen zich manifesteren en op basis daarvan te kijken welke juridische interventie het meest effectief is. Voor wat betreft de afweging tussen *ex ante* regulering of *ex post* regulering biedt het rapport *Spioneren met hobbydrones en andere technologieën door burgers: een verkenning van de privacyrisico's* reeds een stappenplan voor de wetgever.[317] Wij verwijzen graag naar dit schema en hebben het volledigheidshalve hier beneden integraal opgenomen.

[316] Burgers kunnen ook technologie gebruiken om zelf hun privacy beter te beschermen. Denk bijvoorbeeld aan middelen om afluisterapparatuur te detecteren, programma's die spyware of ongeoorloofd netwerkverkeer detecteren en kleding die biometrische systemen misleidt. Wij hebben evenwel geen grootschalige toepassing van deze middelen door burgers gevonden. Verder vallen deze toepassingen buiten de scope van dit onderzoek.
[317] Galic, M. et al. (2020), *Spioneren met hobbydrones en andere technologieën door burgers: een verkenning van de privacyrisico's en reguleringsmogelijkheden, WODC*

Afbeelding 4: Stappenplan regulering spionageproducten

Naast wet- en regelgeving verdient tenslotte zelfregulering en voorlichting aandacht, met name in de online context. Niet alleen is zelfregulering en voorlichting flexibeler dan formele wetgeving, het helpt ook bij het vaststellen en bevestigen van normen en maatschappelijke verwachtingen met betrekking tot privacy in een omgeving die minder receptief is voor wetgeving als normstellend instrument.

In de digitale wereld zijn veel normen en verwachtingen met betrekking tot privacy nog veel minder vast omlijnd. Dit komt allereerst door het feit dat de digitale wereld nog relatief jong is en normen en waarden dus nog weinig tijd hebben gehad om zich te 'zetten'. Daar waar er in de fysieke wereld door de jaren heen bijvoorbeeld duidelijke verwachtingen zijn met betrekking tot privacy, die vaak gekoppeld zijn aan fysieke ruimten (kleedkamers, slaapkamers), zijn deze in de digitale wereld nog niet altijd expliciet.[318] Daarnaast zorgt de snelle technologische vooruitgang er ook voor dat er minder tijd is voor deze normen om zich te bestendigen. Als een norm eenmaal is gevestigd, dan staat er vaak alweer een nieuwe toepassing, techniek of dienst klaar. Tenslotte speelt de relatieve afwezigheid van gezaghebbende instituties een rol bij (het achterblijven) normontwikkeling in de digitale wereld.[319]

Dit alles zorgt ervoor dat formele wetgeving een minder geschikt instrument is om normen te bevestigen. Voorlichting en zelfregulering kunnen helpen bij het vormen en handhaven van normen en waarden in een dynamische omgeving waar de overheid een minder sterke aanwezigheid heeft.

[318] Zie in dit kader: Koops, B. J. (2018), Privacy Spaces, in: *West Virginia Law Review*, Vol. 121, Iss. 2 [2018]
[319] Zie paragraaf 2.3.6

14 Samenvatting en conclusies

Op basis van ons onderzoek komen wij tot de onderstaande samenvatting en conclusies waarin wij antwoord geven op de rechtsvragen die centraal stonden in dit onderzoek:

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

14.1 Horizontale privacy

Het recht op privacy is vastgelegd in internationale mensenrechtenverdragen en onze eigen Grondwet. Het recht op privacy is een klassiek grondrecht dat bovenal zijn werking heeft in de verticale relatie tussen overheid en burgers. Het recht op privacy stelt grenzen aan de inmenging van de overheid in de persoonlijke levenssfeer van de burger.

Het recht op privacy als exponent van de menselijke waardigheid speelt echter ook een rol tussen burgers onderling en tussen burgers en private rechtspersonen. In deze horizontale verhoudingen vinden ook schendingen van het recht op privacy plaats. Horizontale privacy is dus de bescherming van het recht op privacy tussen private personen (rechtsvraag 1).

Het recht op privacy kan op verschillende manieren worden aangetast. In dit rapport maken wij een onderscheid tussen handelingen waarmee inbreuk wordt gemaakt op de persoonlijke levenssfeer en de waarden en belangen die door deze handelingen worden aangetast of in het gedrang komen. Op basis van ons onderzoek komen wij tot de volgende categorisering:

Horizontale privacyschendingen (burger-burger)		
Handelingen	**Verschijningsvormen (voorbeelden)**	**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

In de relatie tussen burgers en private rechtspersonen (meer specifiek het bedrijfsleven) zien we dat met name de verwerking van persoonsgegevens kan leiden tot aantastingen van de persoonlijke levenssfeer. Wanneer een legitieme basis voor de verwerking van deze gegevens ontbreekt, is er sprake van een ongeoorloofde aantasting van de privacy.

Horizontale privacyschendingen (burger-bedrijfsleven)		
Handelingen	**Verschijningsvormen (voorbeelden)**	**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.

Hiermee zijn de rechtsvragen 2 en 3 beantwoord (wat zijn de te beschermen belangen en hoe worden deze aangetast).

14.2 Horizontale privacy en digitalisering

In dit rapport leggen wij de nadruk op 'digitale schendingen' van de horizontale privacy. De reden hiervoor is dat in bijzonder het gebruik van nieuwe technologieën en diensten vragen oproept met betrekking tot de normering van het recht op privacy en de geboden rechtsbescherming. De digitalisering van de samenleving heeft geleid tot een toename van het aantal privacyschendingen in horizontale verhoudingen. Met behulp van producten en diensten die specifiek gericht zijn op het bespioneren van personen (*spycams*, *stalkerware*), maar ook met middelen zoals *smartphones* kunnen mede-burgers eenvoudig worden geobserveerd en gegevens worden vastgelegd.

Internetplatformen en -diensten spelen een belangrijke rol bij horizontale privacyschendingen. De aard van het internet en de diensten van internetplatformen vergroten het effect van digitale privacyschendingen uit. De informatie die geobserveerd en vastgelegd is kan via internetplatformen eenvoudig worden gedeeld. Het effect van het delen van de informatie is tegelijkertijd ook groter omdat een wereldwijd publiek kennis kan nemen van de inbreuk. Internetplatformen en digitale communicatiediensten maken interactie en communicatie ook eenvoudig. Een combinatie van anonimiteit en afstand tot het slachtoffer maakt het dat beledigingen en bedreigen van een ander via sociale media relatief laagdrempelig is. Ook *stalking* en pesten krijgen door digitale communicatie een nieuwe dimensie, alleen al omdat het slachtoffer zich zelfs in de veiligheid van zijn eigen huis niet kan onttrekken aan zijn belagers.

14.3 Horizontale werking van grondrechten

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 kan 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 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 aan 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 AVG) überhaupt de bandbreedte voor het invoeren van een nationaal recht op informationele zelfbeschikking zeer beperkt is.

14.4 Normering en rechtsbescherming horizontale privacy

De bescherming van het recht op privacy krijgt gestalte op grondwettelijk niveau en is nader uitgewerkt in lagere wet en regelgeving zoals het strafrecht, het gegevensbeschermingsrecht, het civiel recht en het administratief recht in Nederland en de door ons onderzochte landen. Een lappendeken van wettelijke bepalingen uit verschillende rechtsgebieden waarborgt het recht op privacy in horizontale verhoudingen. In de hoofdstukken 6 tot en met 9 worden de specifieke bepalingen in detail besproken ter beantwoording van de rechtsvragen 1, 4, 5 en 7. Hierbij valt op dat er relatief weinig aandacht is voor preventie (bijvoorbeeld door middel van verboden op inbreukmakende producenten of diensten, of product- en kwaliteitseisen), alleen in Duitsland hebben wij een (beperkt) verbod op afluisterapparatuur gevonden. De beperkte aandacht voor preventie valt waarschijnlijk te verklaren vanuit het feit dat veel producten en diensten zowel legitieme als illegale toepassingen hebben.

Voor ernstige horizontale privacyschendingen zijn er de bepalingen uit het Wetboek van Strafrecht. Daar waar het gaat om de handelingen observeren en vastleggen zijn er diverse bepalingen op het gebied van

heimelijk cameratoezicht, het afluisteren van gesprekken, het overnemen van gegevens en computervredebreuk. Daar waar het gaat om handelingen als creëren, delen en communiceren zijn met name de uitingsdelicten relevant. Tenslotte geldt dat voor interactie en communicatie onder omstandigheden ook het delict belaging in beeld komt. Sommige schendingen van de horizontale privacy die via het internet plaatsvinden zoals *trolling* of *pranking* zijn niet zelfstandig strafrechtelijk gesanctioneerd. Afhankelijk van de omstandigheden van het geval kunnen dit soort gedragingen echter wel strafbaar zijn, bijvoorbeeld wanneer er sprake is van mishandeling of vernieling.

Wanneer wij kijken naar het gegevensbeschermingsrecht dan zien we dat door het gekozen wetgevingsinstrument (een Verordening) er weinig ruimte is voor nationale afwijking. Bij het gegevensbeschermingsrecht speelt ook de materiële reikwijdte van de wetgeving een rol. Hoewel de AVG ook van toepassing is op natuurlijke personen (zij kunnen verwerkingsverantwoordelijke zijn), is de wet toch grotendeels toegeschreven op rechtspersonen zoals bedrijven en overheidsorganisaties. Verder vallen verwerkingen van een 'zuiver huishoudelijke aard' buiten het toepassingsgebied van de AVG, waardoor bepaalde verwerkingen van persoonsgegevens in horizontale verhoudingen buiten schot blijven. Wel heeft het Europees Hof van Justitie (EHvJ) aangegeven dat wanneer persoonsgegevens in bredere kring worden gedeeld, bijvoorbeeld door ze openbaar op het internet te plaatsen, het gegevensbeschermingsrecht van toepassing is. In de praktijk zien we echter dat handhaving tegen individuen zelden tot nooit voorkomt.

Het algemeen administratief recht is als zodanig van beperkt belang in horizontale verhoudingen. Wel kan het een rol spelen bij de handhaving en naleving van bepaalde normen, bijvoorbeeld via Algemene plaatselijke verordeningen.

Het consumentenrecht en het mededingingsrecht zijn enkel relevant in de horizontale relatie tussen burger en bedrijfsleven. Omdat er in deze context veelal sprake is van een scheve machtsverhouding, kunnen we wellicht beter spreken van de regulering van 'diagonale privacy'. De problematiek van grote bedrijven die de persoonsgegevens van burgers verwerken bevindt zich steeds meer op het snijvlak van het gegevensbeschermingsrecht, het consumentenrecht en het mededingingsrecht. Vooralsnog zijn consumenten- en mededingingsautoriteiten (met uitzondering van Duitsland) relatief terughoudend geweest met het aanspreken van grote (tech)bedrijven op horizontale privacyschendingen.

Burgers kunnen zelf optreden tegen schendingen van hun horizontale privacy via het civiele recht. De actie uit onrechtmatige daad is de belangrijkste mogelijkheid om op te treden tegen horizontale privacyschendingen. Naast een vergoeding van de schade is het ook mogelijk om rectificatie te eisen. Daarnaast kunnen burgers optreden tegen schendingen van hun horizontale privacy op basis van het auteursrecht en het daaraan gerelateerde portretrecht. Maar los van een verbod op publicatie zijn er weinig mogelijkheden om pro-actief tegen horizontale privacyschendingen op te treden.

Hoewel de onrechtmatige daadsactie ruimte biedt om op te treden tegen horizontal privacyschendingen, zijn er toch diverse redenen waarom deze slechts in beperkte mate wordt ingezet. Burgers weten vaak niet dat hun privacy wordt geschonden (bijvoorbeeld door een heimelijk gemaakte foto of video), wie de

eventuele dader is, richten door een rechtszaak nog meer aandacht op dat wat met de privacyinbreuk is onthuld, kunnen juist bij de kleinere privacyinbreuken vaak lastig concretiseren welke schade uit die inbreuken volgt en ontberen voor het aanvechten van grotere inbreuken vaak de nodige expertise, middelen en tijd om een niet zelden langlopende rechtszaak uit te procederen.

14.5 Rechtsvergelijking

Het algemene beeld dat voortvloeit uit de rechtsvergelijking is dat de normering van het recht op privacy in horizontale verhoudingen en de daarbij behorende rechtsbescherming in Nederland niet wezenlijk afwijkt van de wijze waarop deze is vormgegeven in de door ons onderzochte landen.

Het gegevensbeschermingsrecht in de door ons onderzochte landen is nagenoeg gelijk aan dat van Nederland. Zoals hierboven beschreven valt dit te verklaren vanuit de harmonisering van het gegevensbeschermingsrecht op Europees niveau.

De mogelijkheden die het civiel recht biedt om op te treden tegen horizontale privacyschendingen is ook op hoofdlijnen vergelijkbaar. Zo kan er door het instellen van een onrechtmatige daadsactie op vergelijkbare wijze worden opgetreden tegen smaad, laster en andere aantastingen van de eer en de goede naam. Gesteld kan worden dat met betrekking tot landen als Zweden en het Verenigd Koninkrijk het Nederland civiel recht zelfs ruimere mogelijkheden biedt. Daar staat tegenover dat in Nederland de schadevergoedingen beperkt zijn, waardoor een actie vaak niet 'loont', in ieder geval niet in monetaire zin.

De voornaamste verschillen in de normering van horizontale privacyschendingen zitten in het strafrecht. Hoewel de Nederlandse catalogus van delictsomschrijvingen op hoofdlijnen niet veel afwijkt van die in de door ons onderzochte landen, zijn er wel twee relevante bepalingen in het buitenland die wij in Nederland (nog) niet kennen. In Polen en het Verenigd Koninkrijk bestaat een bredere strafbaarstelling voor het verspreiden of toezenden van aanstootgevende content en in Duitsland en Zweden is er een strafbaarstelling voor het filmen van hulpbehoevenden.

14.6 De rol van producenten, distributeurs en internetplatformen

Producenten en distributeurs van producten en diensten en internetplatformen spelen een belangrijke rol bij het faciliteren van horizontale privacyschendingen. Producenten en distributeurs van bijvoorbeeld *spycams* en *stalkerware*, maar ook fabrikanten van smartphones en *Internet of Things* toepassingen, stellen burgers en bedrijven in staat om personen te observeren en hun gegevens vast te leggen. Internetplatformen (sociale media platformen in het bijzonder) spelen een belangrijke rol bij het delen en verspreiden van content en bij de communicatie tussen personen.

14.6.1 Regels voor producenten en distributeurs

Voor bepaalde productcategorieën zoals *spycams*, GPS-peilbakens en *stalkerware* kan gesteld worden dat hun primaire toepassing het maken van inbreuk op de privacy is. Voor andere productcategorieën zoals bijvoorbeeld *smartphones* en *Internet of Things* toepassingen geldt dat zij niet als primaire doel heimelijke observatie hebben, maar dat zij desalniettemin geschikt zijn om privacyinbreuken mee te plegen. Wij hebben geen specifieke regels gevonden met betrekking tot de productie en verkoop van deze

verschillende productcategorieën.[320] Dit omdat het doorgaans afhangt van de toepassing door de gebruiker of er sprake is van een (onrechtmatige) inbreuk op de privacy.

14.6.2 Regels voor internetplatformen

Internetplatformen zijn op grond van de Europese Richtlijn Elektronische handel niet aansprakelijk voor de gedragingen van hun gebruikers wanneer zij geen wetenschap hebben van deze gedragingen en wanneer zij dit wel hebben, prompt handelen om de gewraakte informatie te verwijderen. Internetplatformen kunnen verder ook niet verplicht worden om pro-actief hun platform te monitoren op schadelijke of illegale content.

Voor een effectieve rechtsbescherming zijn de internetplatformen wel cruciaal, omdat zij als enige in staat zijn om hun platformen te reguleren. Naast het verwijderen van content kunnen de internetplatformen gebruikers schorsen of in het geheel verwijderen van hun platform. Ook kunnen zij identificerende gegevens doorgeven aan de autoriteiten of benadeelde burgers. Er is daarom op Europees en nationaal niveau veel discussie over de verantwoordelijkheid van internetplatformen.

In Duitsland geldt het meest strikte regime voor internetplatformen met de Netwerkhandhavingswet (Netzwerkdurchsetzungsgesetz, kortweg NetzDG). Wanneer er sprake is van illegale content dan moet deze na een melding binnen 24 uur verwijderd zijn. In Zweden bewijst een oude wet voor de aansprakelijkheid voor bulletinboard (BBSen) nog steeds dienst. Deze wet verplicht houders van digitale berichtendiensten (waar sociale media ook onder vallen) om de nodige zorg te betrachten en onrechtmatige content te verwijderen van het platform.

14.6.3 Zelfregulering, onderwijs en voorlichting

Samenwerkingsvormen tussen burgers, bedrijven en overheid om horizontale privacyschendingen tegen te gaan zien met name op zelfregulering, onderwijs en voorlichting (rechtsvraag 6). Internetplatformen reguleren hun platformen via de gebruiksvoorwaarden en de daarbij behorende *community standards*. In deze standaarden is uiteengezet welke content acceptabel is en welke niet. Platformen kunnen zelfstandig besluiten om content te verwijderen (al dan niet geautomatiseerd) of naar aanleiding van een melding.

Internetplatformen en andere internetdienstverleners werken ook in publiek-privaat verband aan zelfregulering. De meeste zelfregulering is gericht op het bestrijden van illegale content zoals beelden van kindermisbruik, *hate speech* en terroristische content. Voor het tegengaan van minder ingrijpende schendingen van de horizontale privacy zoals de publicatie van privé-informatie of een eenvoudige belediging, hebben wij geen publiek-private initiatieven gevonden.

Op het gebied van voorlichting en onderwijs zijn er in alle onderzochte landen activiteiten gericht op het vergroten van de digitale weerbaarheid van burgers. Veel van de voorlichting die raakt aan de horizontale privacy, is gericht op ouders en kinderen. Via Europese netwerken en initiatieven zoals *Safer Internet* en *Better Internet for Kids* worden kinderen en hun ouders voorgelicht over verantwoordelijk internetgebruik.

[320] In Duitsland is er een verbod op afluisterapparatuur, maar dat strekt zich niet uit tot deze productcategorieën.

14.7 Inpassen van buitenlandse rechtsfiguren in de Nederlandse rechtsorde

Op basis van het bovenstaande kunnen we concluderen 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 (rechtsvraag 8 en 9).

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 voor de overheid om autonoom normstellend en handhavend op te treden. Een groot risico van 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 schadelijk is, 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 effect waarmee rekening moet worden gehouden is dat beelden van omstanders ook kunnen bijdragen aan de opheldering van een misdrijf of het vaststellen van de toedracht van een ongeluk. Hier moet bij een eventuele strafbaarstelling ook 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. Het is van belang om in dit kader nauwgezet de ontwikkelingen in Brussel te volgen, nu het Europese aansprakelijkheidsregime voor internettussenpersonen op het moment van schrijven wordt herzien.

14.8 Bepalingen die de horizontale privacy versterken, niet ontleend aan het buitenland

Naast het inpassen van buitenlandse bepalingen kunnen ook nog enkele voorstellen worden gedaan die niet 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 kan gedacht worden 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 zou kunnen worden onderzocht 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. Gesteld kan worden dat met de *privacy by design* eis uit artikel 25 AVG er al deels een wettelijke basis bestaat om dergelijke maatregelen af te dwingen.

Meer in het algemeen kan worden gesteld dat de wetgever juist in de digitale omgeving moet investeren in mechanismen om technologische ontwikkelingen, nieuwe toepassingen en de mogelijke consequenties daarvan vroegtijdig te signaleren. Als met wetgeving een aantal jaar wordt gewacht, dan is de techniek vaak al verouderd op het moment dat een nieuwe wet(sbepaling) van kracht wordt of, als dat niet het geval is, dan kan een techniek of toepassing al zo wijdverbreid en veelgebruikt zijn dat het vrijwel onmogelijk is om daar nog wezenlijke grenzen aan te stellen. Het faciliteren van permanente monitoring en maatschappelijke discussie, bijvoorbeeld via de instelling van een vaste Kamercommissie, kan bijdragen aan het vroegtijdig signaleren en vervolgens reguleren van nieuwe privacyschendingen.[321]

14.9 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 aldus 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.

Gezien de beperkingen van formele wet- en regelgeving voor het normeren en reguleren van digitale privacyschendingen is het ook van belang te kijken naar voorlichting en zelfregulering als mechanismen voor het vormen en handhaven van normen en waarden op plaatsen waar de overheid een minder sterke aanwezigheid heeft.

[321] In het verleden was er een tijdelijke Kamercommissie Digitale Toekomst.

15 Literatuurlijst

Akerlof, G. (1970). The market for 'lemons': Quality uncertainty and the market mechanism. In: *The Quarterly Journal of Economics,* 84(3), 488–500.

Alberdingk Thijm, C. (2000), *Privacy versus auteursrecht in een digitale omgeving*, ITER reeks

Allen, A. L. (2011), *Unpopular privacy. What must we hide?,* Oxford: Oxford University Press, 2011

Bogdan, M. (2000), *Swedish Law in the New Millennium*, Nordstets Juridik

Boyd, D. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (Ed.), *A networked self: Identity, community, and culture on social network sites* (pp. 39–58). New York: Routledge.

Brüggemeier, G, Colombi Ciacchi, A., O'Calllaghan, P. (2010), *Personality Rights in European Tort Law (The Common Core of European Private Law) 1st Edition*, Cambridge University Press

Cals, J.M.L.Th., Donner, A. M. (1971), Eindrapport van de Staatscommissie van Advies inzake de Grondwet en de Kieswet', Den Haag, Staatsuitgeverij, via: http://resources.huygens.knaw.nl/watermarker/pdf/cc/scans/1967a_cie_cals-donner/verslag/plenair/data/1971-03-29/1971-03-29.pdf

Cleiren, C. P. M, Ten Voorde, van Waas W. (2019), Strafbaarstelling van sexchatting en sextortion onder de loep. De meerwaarde van een empirisch perspectief, in: *Strafblad*, nummer 2, mei 2019 / SDU

Cocking, D., Van den Hoven, J. (2018) *Evil Online*, Blackwell Wiley

Commissie Grondrechten in het Digitale Tijdperk (2000), *Rapport van de Commissie Grondrechten in het Digitale Tijdperk,* (Commissie Franken)

Custers, B. (2018), Aansprakelijkheid voor drones, in: *Maandblad voor Vermogensrecht* 2018, nummer 7-8, p. 238.

de Vos, B. J. (2010), *Horizontale werking van grondrechten. Een kritiek,* Universiteit Leiden

de Vries, U.R.M.Th., Tigchelaar, H., van der Linden, M., Hol, A.H. (2007), *Identiteitsfraude een afbakening: een internationale begripsvergelijking en analyse van nationale strafbepalingen*, WODC 1496

Dierlamm, A., Cordes M. (2018), § 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen, in: K.D. Scheurle & T. Mayen (red.) *Scheurle/Mayen Telekommunikationsgesetz Kommentar*, 2018, A., para 1

Echikson, W., Knodt, O. (2018) *Germany's NetzDG: A key test for combatting online hate*, CEPS Research Report, no. 2018/09, November 2018, 1-2.

Ekker. A. (2004), Annotatie bij Hof Amsterdam 24 juni 2004 (Pessers/Lycos II), in: JAVI 2004-5.

Engelhard, E. (2019), Ruimer baan voor smartengeld bij inbreuken op fundamentele rechten? Een reactie op HR 15 maart 2019, ECLI:NL:HR:2019:376, via: http://blog.ucall.nl/index.php/2019/03/ruimer-baan-voor-smartengeld-bij-inbreuken-op-fundamentele-rechten-een-reactie-op-hr-15-maart-2019-eclinlhr2019376/

Engelhard, E.F.D. (2019) Immateriële schade als gevolg van data-inbreuken: het ondergeschoven kindje van de AVG, in: *Nederlands Tijdschrift voor Burgerlijk Recht*, volume 9/10, pp. 192 - 200

European Data Protection Supervisor (2014), Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014

Galic, M., Noorman, M. van der Sloot, B., Koops, B. J., Cuijpers, C. Gellert, R., Keymolen, E., Delden, T. (2020), *Spioneren met hobbydrones en andere technologieën door burgers: een verkenning van de privacyrisico's en reguleringsmogelijkheden*, WODC

Gerards, J. (2019), *General principles of the European Convention on Human Rights*

Goffman, E. (1959), *The Presentation of Self in Everyday Life*, New York: Doubleday

Groep gegevensbescherming Artikel 29, *Opinion 5/2009 on social networking*, 01189/09/EN WP 163

Groothuis, M. M. (2019) Tekst en Commentaar Grondwet

Hamer, J. & L. Kool (red.) (2018). *Beschaafde Bits – Zeventien experts over fatsoenlijk digitaliseren*. Den Haag: Rathenau Instituut

Heuchemer, P. (2020), 'StGB § 201a Verletzung Des Höchstpersönlichen Lebensbereichs Durch Bildaufnahmen' in v Heintschel-Heinegg (ed), *BeckOK StGB* (45th edn, 2020) 4.

HM Government, *Online harms White Paper*, April 2019

Keats Citron, D. (2019), Why sexual privacy matters for trust, University of Maryland Legal Studies Research Paper No. 2019-02

Keymolen, E., Noorman, M., van der Sloot, B., Cuijpers, C., Koops, B. J., Zhao B. (2020), *Op het eerste gezicht: Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties*, WODC projectnummer 2992

Kool, R. S. B., Tekst & Commentaar Strafrecht, Pornografie bij: Wetboek van Strafrecht, Artikel 240 [Afbeelding of voorwerp aanstotelijk voor de eerbaarheid]

Koops, B. J. (2018), Privacy Spaces, in: *West Virginia Law Review*, Vol. 121, Iss. 2 [2018]

Koops, B.J., Newell B. C., Roberts A, Škorvánek, I., Galič, M. (2018), The reasonableness of remaining unobserved. A comparative analysis of visual surveillance and voyeurism in criminal law, in: *Law & Social Inquiry*, 18 January 2018, DOI: 10.1111/lsi.12348

Kühl, K., Heger, M. (2014) Strafgesetzbuch: Kommentar, Beck-Online, StGB §243, Rn. 21.

Leidraad van de Raad voor de Journalistiek December 2019

Lindenbergh, S. D. (1999), De Positie en Handhaving van *Persoonlijkheidsrechten* in het Nederlandse Privaatrecht, in: *Tijdschrift voor Privaatrecht*, pp. 1665–1707

Maras, M. H., Alexandrou, A. (2019), Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos, in: *International Journal of Evidence and Proof*, Volume: 23 issue: 3, page(s): 255-262

Młynarska-Sobaczewska, A. *et al.* (eds) (2015), *Horyzontalne oddziaływanie Konstytucji Rzeczypospolitej Polskiej oraz Konwencji o ochronie praw człowieka i podstawowych wolności*, Biuro Trybunału Konstytucyjnego

Mouton, L. (2018), *Hate Speech op Facebook en Twitter: het verwijderen van berichten en accounts versus de vrijheid van meningsuiting*, Universiteit Gent

Nehmelmann, R. (2002), *Algemeen Persoonlijkheidsrecht: een rechtsvergelijkende studie naar het algemeen persoonlijkheidsrecht in Duitsland en Nederland*, Deventer: Wolters Kluwer

Nissenbaum, H. (2004), Privacy as contextual integrity, in: *Washington Law Review*, 79(1), 119-157

Pape, S. (2006), De betekenis van het Jetblast-arrest voor de waarschuwing in het productaansprakelijkheidsrecht, in: *NTBR* 2006, 56, p. 374-382

Penney, J. (2020), Privacy and Legal Automation: The DMCA as a Case Study, in: Stanford Technology Law Review, Vol. 22, No. 1, 412

Quint, P. E. (201), A return to Lüth, in: *Roger Williams University Law Review*, Volume 16, Issue 1

Rainey, B., Wicks, E., Ovey, C, (2002), Jacobs, White and Ovey: The European Convention on Human Rights, Seventh Edition

Regan, P.M. (1995) Legislating Privacy: Technology, Social Values and Public Policy, Chapel Hill: University of North Carolina Press.

Rodrigues, P. R. (2008), *Monitor Racisme & Extremisme*, 8e rapportage, (red. van Donselaar, J. en Rodrigues, P. R.), Pallas Publications, Amsterdam University Press, p. 244

Roosendaal, A. P. C. (2007). Elimination of anonymity in regard to liability for unlawful acts on the internet, in: *International Journal of Technology Transfer and Commercialisation*, *6*(2/3/4), 184-195.

Rosen (2004), *The Naked Crowd*, New York: Random House

Schermer, B. W. Hagenauw, D. Falot, N., (2018) *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*, Ministerie van Justitie en Veiligheid

Staatscommissie Grondwet (2010), *Rapport Staatscommissie Grondwet*

Starnecker, 'BDSG § 4 Videoüberwachung Öffentlich Zugänglicher Räume' in: Gola and Heckmann (eds), *Bundesdatenschutzgesetz* (13th edn, 2019) 1

Steinberg, S. B. (2017), Sharenting: Children's privacy in the age of social media, in: *Emory Law Journal*, vol 66-839, p. 839-884

Thaler, R., Sunnstein, C. (2008), *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Yale University Press

Tworek, H., Leerssen, P. (2019) *An Analysis of Germany's NetzDG Law, A working paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression*, 2019, p. 6.

Ullrich, C. (2017) *Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective*, JIPITEC

van der Jagt, F. (2013), Het recht op bescherming van persoonsgegevens', in: Gerards e.a.(red), Grondrechten. De nationale, Europese en internationale dimensie, Nijmegen: Ars Aequi

Van der Pot, 'Handboek van het Nederlandse staatsrecht', vijftiende druk

van der Sloot, B. (2015), Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system, in: *The Computer Law & Security Review*, 2015-1, p. 26-45.

van der Sloot, B. (2017), *Decisional privacy 2.0: the procedural requirements implicit in Article 8 ECHR and its potential impact on profiling*, in: *International Data Privacy Law*, Volume 7, Issue 3, 1 August 2017.

van der Sloot, B., Schendel (2019), *De Modernisering van het Nederlands Procesrecht in het licht van Big Data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving,* WODC Projectnummer 2900

Kortmann, C. A. J. M. (2016), *Constitutioneel recht*, 7e druk, Deventer: Kluwer

Verheij, A. J. (2002), *Vergoeding van immateriële schade wegens aantasting in de persoon, Nijmegen: Ars Aequi*

Verheul, J. M., Tekst & Commentaar Strafrecht, Valsheid in geschrift bij: Wetboek van Strafrecht, Artikel 225 (laatst geraadpleegd 26 mei 2020)

Verhey, L. (1992), *Horizontale werking van grondrechten, in het bijzonder het recht op privacy*, Tjeenk Willink

Wagner (2017), 'BGB § 824 Kreditgefährdung', in: *Münchener Kommentar zum BGB* (7th edn, 2017) 3.

Westin, A.F. (1967). *Privacy and Freedom*, New York: Atheneum Press

16 Bijlagen

16.1 Bijlage 1: Samenstelling begeleidingscommissie

Evert Stamhuis – Erasmus Universiteit Rotterdam (voorzitter)
Henk van der Veen – WODC
Just Stam – Ministerie van Justitie en Veiligheid
Youetta Visser – Yfactor
Aline Klingenberg – Universiteit Groningen

16.2 Bijlage 2: Deelnemers expertbijeenkomst

Vincent Böhre -Privacy First
Anton Ekker - Ekker Legal
Lotte Houwing - Bits of Freedom
Edo Haveman – Facebook
Willem Korthals Altes - Vereniging voor Media- en Communicatierecht
Floris Kreiken – Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Inger Sanders – Autoriteit Persoonsgegevens
Otto Volgenant – Boekx Advocaten
Tijmen Wisman – Vrije Universiteit / Platform Burgerrechten

16.3 Bijlage 3: Landenrapport Duitsland

Auteur: Ivan Skorvanek

Part 1: Introduction

Legal system

Germany is one of the principal Civil law tradition jurisdictions. Its legal culture, legislative strategies and Constitutional Court judgements has had a great influence on other jurisdictions in the region, especially in Central Europe (German speaking world, CEE countries), but also for instance Italy. German legal tradition is code-based, principal legal fields are codified and the regulatory culture is focused on laws (often very detailed legal regulations compared with other countries). Germany is comprised of Federal States which have relatively wide-ranging legislative powers, supplementing the laws adopted on the federal level (for this report, it is feasible to study the federal level only, various state-level regulations may be mentioned incidentally, if relevant). German legal culture highly values the concept of human dignity, which is enshrined in Art. 1 of the Constitution (*Grundgesetz*). The German Constitution also contains the so-called *Ewigkeitsklausel* (Art. 79(3) of the Constitution), which declares certain principles to be immune to change. According to this clause, no constitutional amendment may be introduced which would alter Art. 1 of the Constitution (protecting human dignity and acknowledging human rights as directly enforceable law), Art. 20 of the Constitution (setting out the republican form of government, democratic character of the state with a separation of powers, federative structure with guaranteed powers of the states, the welfare state and the rule of law) and the separation of powers between the federal and the state governments and legislative bodies.

A typical feature of the German legal system is the very strong role of the Federal Constitutional Court (*Bundesverfassungsgericht*), which has over the years assumed a very important role in re-interpreting existing provisions of the Constitution, especially the fundamental rights provisions, to adapt them to new developments, essentially creating new rights (not explicitly formulated in the constitutional text, but by the interpretation of the existing provisions).
Germany does not have a general Ombudsman office, although various sectoral Ombudsman offices operate. The nearest to an Ombudsman service is the Parliamentary Petitions Committee (*Petitionsausschuss Deutscher Bundestag*), which receives and investigates complaints of maladministration.

Fundamental rights framework

Horizontal effect of constitutional law

German Constitution does not explicitly include the right to privacy and data protection. These rights are derived from other more general rights, in particular from human dignity (Art. 1) and from the free development of personality (Art. 2). The privacy of communications (Art. 10) and the inviolability of the home (Art. 13) are protected explicitly. Art. 1(3) of the German Constitution stipulates that these (and other) rights are directly applicable law, binding to the legislature, the executive and the judiciary.

The idea that constitutional rights have a horizontal effect is widely accepted.[322] There is a number of theories on how this takes effect, the main ones being the indirect horizontal effect and the direct horizontal effect. The theory of indirect horizontal effect is acknowledged by the Federal Constitutional Court (landmark *Lüth* judgement).[323] Indirect horizontal effect means that the constitutional rights influence the interpretation of all other laws (including private law), and can even lead to interpretation against the literal formulation of the law.[324] The ruling ideas of the Basic Law are supposed to radiate to all areas of law.[325] When applying norms of private law, a judge must take into account their possible modifications influenced by constitutional norms.[326] The theory of direct horizontal effect attributes the influence of constitutional rights in horizontal relations to their character as objective and binding constitutional law, thus not only affecting the interpretation of private law norms, but directly giving basis for subjective individual rights.[327] A third theory of rights against the state emphasizes that the state has made the private law and enforces it, and therefore must take responsibility even for infringements of private parties.[328]

Personality rights and fundamental rights protection

The general personality right in Constitutional Law is derived from the right to individual freedom (Art. 2(1) of the Constitution) in conjunction with the inviolability of human dignity (Art. 1 of the Constitution).[329] The content of this right is one of the most elusive in the Constitution. Ultimately, a bundle of individual personality forms is protected, which have been recognised to receive specific protection. What connects them is the aim to protect and maintain personal integrity.[330] In German Constitutional Law, the general personality right functions as a sort of gap-filler, guaranteeing elements of personality that are not protected by any special provisions of the Constitution, which does not make them inferior to those that are.[331] The Federal Constitutional Court sets the general personality right apart and in opposition to the active general freedom of action (also protected by Art. 2 of the Constitution). The general personality right is a right to respect a definable protected space from the active element of this development.[332] In the constitution this is also expressed in Art. 2: "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others".

German law rarely uses the term privacy. The so-called Spheres Theory (Spären theorie) is often used to contour general personality rights.[333] According to the Spheres Theory, a distinction can first be made between an inner sphere, which also marks individual identity on the one hand, and an outer sphere, which encompasses social identity, on the other. Within the former, it will again be necessary to differentiate between the - in principle untouchable - intimate sphere and the private sphere in its manifold forms. Informational self-determination (from which personal data protection is derived) lies across these three spheres.[334] Although it does not appear that a victim can directly draw on the violation of the constitutional

[322] Robert Alexy, A Theory of Constitutional Rights, Oxford, 2010, 354.
[323] *Lüth* judgement. Federal Constitutional Court, Judgement of the first senate 15. January 1958, 1 BvR 400/51. ECLI:DE:BVerfG:1951:rs19580115.1bvr040051.
[324] *Lüth* judgement.
[325] *Zwangsversteigerung I* judgement. Federal Constitutional Court, Judgement of the second senate 24. March 1976, 2 BvR 804/75.
[326] *Lüth* judgement.
[327] Robert Alexy, A Theory of Constitutional Rights, Oxford, 2010, 356.
[328] Robert Alexy, A Theory of Constitutional Rights, Oxford, 2010, 356.
[329] Hannes Rösler, 'German Privacy Rights under European Influence' in Bettina Heiderhoff and Grzegorz Zmij (eds.), *Tort Law in Poland, Germany and* Europe, sellier, 2009, 36.
[330] Lang, 'GG Art. 2 [Persönliche Freiheitsrechte]' in Epping and Hillgruber (eds), *BeckOK Grundgesetz* (42nd edn, 2019) 32.
[331] ibid 34.
[332] *Eppler* judgement. Federal Constitutional Court, Judgement of the first senate 3. June 1980, 1 BvR 185/77.
[333] Lang (n 11) 35.
[334] ibid 38.

rights (only on the provisions that codify them in statutes), the courts are obliged to interpret all provisions of the law in conformity with the essence of these rights (indirect horizontal effect, see supra 2.1).

Extra legem, intra ius

The general personality right itself is not explicitly formulated, but developed by the Federal Constitutional Court. Its exact contours are left purposefully vague and the list of rights derived from the general personality right is open to further development. Thus, the Federal Constitutional Court developed the doctrine of inviolable core of personality[335] or the right to integrity and confidentiality of computer systems[336] (though these are for the moment largely confined to state-citizen relationships). More relevant for the horizontal relations was the development of the right to informational self-determination which guarantees the individual's authority to determine, in principle, themselves about the disclosure and use of their personal data.[337] In the intimate sphere, an example of special right is the protection of personal secrets such as diary records (as addressee-free written records)[338], but also the right to choose a gender identity[339] and sexual self-determination[340]. Rights in the social sphere are numerous, for example a right to one's own image[341], right to one's own (spoken) word (individual's ability to fully disclose feelings, to freely express judgment about relationships and people)[342], right to one's own name[343], protection of honour and against defamation[344] and the right to personal reputation[345].

Relevant case law (national)

The most important cases concerning this field were the *Lüth* case, in which horizontal effect of constitutional rights was established and the judgment on the constitutionality of the Census Act which 'created' the right to informational self-determination (other cases were referenced throughout the previous sections).

Lüth case - Federal Constitutional Court, Judgement of the first senate 15. January 1958, 1 BvR 400/51. ECLI:DE:BVerfG:1951:rs19580115.1bvr040051

The judgment is by some considered the "most powerful decision" of the court.[346] Lüth called for a boycott of a film directed by a former "nazi director". The production company sued him for a violation of common

[335] Federal Constitutional Court, Judgment of the first senate from 16 January 1957, 1 BvR 253/56, Rn. 32. ECLI:DE:BVerfG:1957:rs19570116.1bvr025356.

[336] *Grundrecht auf Computerschutz* judgement, Federal Constitutional Court, Judgment of the first senate from 27 February 2008, 1 BvR 370/07. ECLI:DE:BVerfG:2008:rs20080227.1bvr037007.

[337] *Volkszählung* judgement, Federal Constitutional Court, Judgment of the first senate from 15. December 1983, 1 BvR 209/83. ECLI:DE:BVerfG:1983:rs19831215.1bvr020983.

[338] *Tagebuch* judgement, Federal Constitutional Court, Judgment of the second senate from 14 September 1989, 2 BvR 1062/87.

[339] Federal Constitutional Court, Judgment of the first senate from 10 October 2017, 1 BvR 2019/16, Rn. 37. ECLI:DE:BVerfG:2017:rs20171010.1bvr201916

[340] Transsexuelle V judgement, Federal Constitutional Court, Judgment of the first senate from 27 May 2008, 1 BvR 10/05.

[341] Federal Constitutional Court, Judgment of the first chamber of the first senate from 14 February 2005, 1 BvR 240/04. ECLI:DE:BVerfG:2005:rk20050214.1bvr024004.

[342] Federal Constitutional Court, Judgment of the first senate from 9 October 2002, 1 BvR 1611/96. ECLI:DE:BVerfG:2002:rs20021009.1bvr161196.

[343] *Mißbrauchsbezichtigung* judgement, Federal Constitutional Court, Judgment of the first senate from 24 March, 1 BvR 131/96. ECLI:DE:BVerfG:1998:rs19980324.1bvr013196.

[344] Federal Constitutional Court, Judgment of the first senate from 16 August 2002, 1 BvR 1241/97. ECLI:DE:BVerfG:2002:rk20020816.1bvr124197.

[345] Federal Constitutional Court, Judgment of the first senate from 17 September 2012, 1 BvR 2979/10. ECLI:DE:BVerfG:2012:rk20120917.1bvr297910.

[346] Matthias Jestaedt: *Meinungsfreiheit*. In: Detlef Merten, Hans-Jürgen Papier (Eds.): *Handbuch der Grundrechte in Deutschland und Europa*. Band 4: *Grundrechte in Deutschland. Einzelgrundrechte I.* C. F. Müller, Heidelberg, 2011, 876.

decency under the Civil Code (BGB) and lower level courts decided against him. However, the Federal Constitutional Court declared that his actions were protected by his freedom of expression (Art. 5 of the Constitution). The Federal Constitutional Court declared fundamental rights to act as an objective value even in civil proceedings (the so-called radiation effect), meaning that the civil law provisions must be interpreted in conformity with the fundamental rights and weighing up of competing goods in light of the constitutional norms must be undertaken.

Decision on the Constitutionality of the Census Act - Federal Constitutional Court, Judgement of the first senate from 15. Dezember 1983, 1 BvR 209/83. ECLI:DE:BVerfG:1983:rs19831215.1bvr020983 (https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html)
The proceedings concerned a number of constitutional complaints challenging the 1983 Federal Census Act which provided for comprehensive collection of personal data of citizens. In its judgement, the Court developed the right to informational self-determination, as a fundamental rights guarantee that gives an individual the right to decide themselves on the disclosure and use of their personal data. Limitations of this right are only permitted, if there is an overriding public interest.

The role of providers and distributors

In this field, the most discussed development in Germany has been the Network Enforcement Act (*Netzwerkdurchsetzungsgesetz*), also entitled as the Act to improve enforcement of the law in social networks. (English translation of the law available here: https://germanlawarchive.iuscomp.org/?p=1245)
The stated aim of this law was to improve the compliance with the law on social media, through deletion of criminal contributions on social networks, and in this way to ensure a free, open and democratic culture of communication and the protection of groups and individuals affected by hate crimes.
The Act is applied to for profit service providers operating internet platforms enabling users to share any content with other users and make such content available to the public. Social networks which have fewer than two million registered users in Germany are exempted from the obligations set out by this law.
The unlawful social media content targeted by the law is a list of criminal offences from the Criminal Code, mainly concerning hate speech, promotion of extremism and terrorism, but also (more relevant for the purposes of this report) criminal offences of insult, malicious gossip and defamation (for more on these criminal offences see *infra* 6.1), and also various threats.
Two principal kinds of obligations are established by the law for the social media companies. Section 2 requires them to twice a year report (if they receive at least 100 complaints annually) how they handled the complaints about unlawful content on their platforms. Section 3 provides the rules for handling the complaints. These social networks must create an accessible tool for all users to report unlawful content. If such report is made, manifestly unlawful content must be deleted or blocked within 24 hours, although no definition is provided on what 'manifestly unlawful content' is. In this way, the private companies must make their own judgement on lawfulness or unlawfulness of the content. In case the unlawfulness of the content has to be determined (for instance factuality of the content needs to be checked), the period to delete or block content is extended to 7 days. In case content is removed, it should be preserved as evidence of unlawful behaviour for a period of ten weeks. Under Section 4, a failure to comply with the duties described in this paragraph can be subject to a fine of up to 5 million Euros (in 2019, for instance, Facebook was fined 2 million Euros under the Network Enforcement Act, see *infra* Section 7.6). Importantly, the law establishes extraterritorial effect, and the regulatory offence may be sanctioned even, if it is not committed in Germany.

Critics view the new law as an attempt to privatise a new censorship regime, forcing social media platforms to respond to this new painful liability with unnecessary takedowns. However, a study by CEPS indicated that Network Enforcement Act "has not provoked mass requests for takedowns. Nor has it forced internet platforms to adopt a 'take down, ask later' approach." Removal rates among the big three platforms ranged from appr. 10-20%.[347] Yet, it is unclear whether the proponents of the law have been right in their expectations either. Evidence suggests that social media companies rather rely on their own community standards when tackling problematic content, and only check compliance with the Network Enforcement Act in the second step. In this light, the true effect of the law may be a swifter and more consistent removal of content under social networks' own community rules within Germany.[348]

Part 2: Protection of privacy and data in horizontal relations

In this part we want to explore how privacy and data protection in horizontal relations is effectuated through specific legislation.

Data protection legislation

Relevant articles and rationale

German personal data protection tradition is one of the longest in the world. The first data protection law was adopted in 1970 by the Hesse state, the first Federal Data Protection Act (*Bundesdatenschutzgesetz*) was adopted in 1979. With the entry into force of the GDPR a new Federal Data Protection Act (further: BDSG) also entered into force on the same day. Available in English here: https://www.gesetze-im-internet.de/englisch_bdsg/ The German legislature took advantage of several open clauses in the GDPR to introduce a number of distinctive elements. This section will briefly introduce the main differences between the BDSG and the GDPR. Since most of these differences are procedural in nature or introduce further derogations, they will not be discussed in detail, except for the special provision on video surveillance of public spaces which is peculiar to German data protection law.

Appointment of data protection officers: Section 38 BDSG introduces stricter requirements to appoint a data protection officer (they must be designated, if the company employs at least 10 persons dealing with automated processing of personal data, or undertakes data processing subject to DPIA under the GDPR).

Processing special categories of data: BDSG contains broad implementation of the exceptions found in Art. 9(2)(b)(h)(i)(j) of the GDPR.

Processing criminal conviction data: BDSG does not contain a provision allowing processing of criminal conviction data by non-state actors, except in the employment context (Section 26(1) BDSG: if "The employer has a documented reason to believe that the data subject committed a crime while employed").

Processing for secondary purposes: BDSG allows this beyond what GDPR permits, for example Section 24(1) BDSG (for the establishment, exercise or defense of legal claims).

Child consent age requirement: Not lowered by the BDSG.

Variations in data subject rights: including information right, access right, data breach notification, erasure right.

[347] William Echikson, Olivia Knodt, Germany's NetzDG: A key test for combatting online hate, CEPS Research Report, no. 2018/09, November 2018, 1-2.

[348] Heidi Tworek, Paddy Leerssen, An Analysis of Germany's NetzDG Law, A working paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 2019, 6.

Further rules for derogations for specific processing situations: Processing for scientific and historical, or statistical research, secrecy obligations, processing in the employment context.
Non-monetary damages: BDSG defines non-monetary damages which can be claimed by data subjects.
Video surveillance: BDSG contains a special provision (Section 4) on video surveillance of publicly accessible places. This shall only be allowed to either public bodies to perform their tasks, or to determine who shall be allowed or denied access or to safeguard legitimate interests for specifically defined purposes, and if there is nothing to indicate legitimate overriding interests of the data subjects. This provision was retained from the previous BDSG with little change. Its purpose was to create a specific legal basis for video surveillance, against the background that the GDRP contains only general data processing clauses.[349] It is, however, not clear whether the provision is permissible under the GDPR, which takes precedence over the national regulation. Expressly retaining it after GDPR adoption shows that the legislature expects the provision to have a purpose, however, literature is skeptical.[350]

Case law

The current legal framework is only in place for a relatively short time and it is yet to be seen how the courts will deal with its application. Worth mentioning here is the very recent decision of the Higher Regional Court in Berlin which declared various aspects facebook's term and conditions to be incompatible with data protection and consumer law.

Higher Regional Court in Berlin (*Kammergericht Berlin, 5. Zivilsenat*), Decision from 20.12.2019 - 5 U 9/18, ECLI:DE:KG:2019:1220.5U9.18.0A.

The case was originally brought by a consumer protection organization against Facebook, and appealed by both parties after the initial lower court decision. The lower court decision was largely upheld by the Higher Regional Court. The motion of the plaintiff that the statement "Facebook is and remains free" is false advertisement because users pay with their data was rejected by the court (margin 58). However, the other parts of the plaintiff's complaints against Facebook were largely upheld. In particular:

- The so-called blind consent required of Facebook users is not in compliance with data protection law.
- The data collection made possible by default settings is not necessary for the implementation of a legal obligation with the user, it may be useful and helpful, but is not necessary (margin 39).
- The default revealing of the location of the user, and access of search engines to the content of the user feed are also not necessary (margin 50), and the user did not explicitly provide consent for such collection.
- Also not acceptable is the notice that names and profile pictures of users may be used for further content

Actions by the supervisory authority

Germany does not have one central Data Protection Authority, but 16 different authorities in the German states that are responsible for enforcing the data protection regulations (EU, Federal and

[349] Starnecker, 'BDSG § 4 Videoüberwachung Öffentlich Zugänglicher Räume' in Gola and Heckmann (eds), *Bundesdatenschutzgesetz* (13th edn, 2019) 1.
[350] Wilhelm, 'BDSG § 4 Videoüberwachung Öffentlich Zugänglicher Räume' in Wolff and Brink (eds), *BeckOK Datenschutzrecht* (31st edn, 2019) 1.

also state data protection acts). On the federal level, the Federal Commissioner for Data Protection and Freedom of Information is established, but generally only has authority over public bodies, which are beyond the scope of this report, as is a systematic study of all 16 state authorities. To make sure the same approach to data protection is taken throughout Germany, the state authorities have established the Data Protection Conference (Datenschutzkonferenz) consisting of all 16 authorities to coordinate their approach. An example of such coordination is the October 2019 set of guidelines on how to determine the amount of fines for violation of the GDPR:https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf

To give a recent example of enforcement in line with these guidelines, on 30 October 2019, the Berlin DPA issued a fine of 14,5 million Euro to Deutsche Wohnen SE (a large real-estate company) for unjustified retention of customer data.[351] The company was accused of storing personal data of tenants in a manner which did not allow erasure of data that was no longer necessary, including personal and financial circumstances in the forms of payslips, employment contracts, tax data, social security and health insurance data, and bank statements. Such archiving without possibility of erasure and often without legal grounds for collection was found to be an infringement of the data protection by design requirements under Art. 25 GDPR as well as general principles under Art. 5 GDPR.

Significance in practice

It is perhaps too early to assess whether the goal of the regulation has been reached. Literature is skeptical on various points about the BDSM being in compliance with the GDPR, and is awaiting how the courts will deal with it (these points are generally not of much relevance for this report). Some enforcement actions, such as those mentioned in sections 4.3 and 4.2 show that German regulators in the field of Data Protection are willing to enforce Data Protection laws against large corporations and to issue fines in significant amounts. Whether this will lead to higher compliance is yet to be seen.

[351] '20191105-PM-Bussgeld_DW.Pdf' <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf> accessed 14 March 2020.

Administrative, anti-trust and consumer protection law

Relevant articles and rationale

German administrative law generally establishes vertical relations of citizens and state authorities. For this reason, the connection of administrative law to horizontal privacy is rather limited. A relevant connection can be made with regard to various administrative offences, partly included in the Act on Regulatory Offences (*Gesetz über Ordnungswidrigkeiten*), partly scattered across various sectoral laws. The offences under the Act on Regulatory Offences, for which the sanction is an administrative fine, include for instance the following (with connection to a broadly understood concept of privacy):

Public instigation of offences (Section 116), Inadmissible Noise (Section 117) without a justified reason creating a considerable disturbance, Public Nuisance (Section 118), i.e. grossly offensive acts, Grossly offensive and disturbing acts (Section 119) i.e. public act or dissemination of writing, sound carriers, video or pictures of sexual acts, or sexual act in a place where this is grossly offensive.

Examples of sectoral regulation include the Federal Control of Pollution Act (*Bundesimmissionsschutzgesetz*) which regulates various form of pollution including noise, air pollution (these have been considered privacy violations by the ECtHR), etc. Another example is the German Fiscal Code (*Abgabenordnung*) establishing tax secrecy in Section 30 and following. Although this is primarily binding the public authorities, it also applies to officially consulted experts. Breach of tax secrecy is a criminal offence, the relevance of administrative law is that is defines who and under what conditions has a duty to respect tax secrecy. Administrative law also establishes exceptions, such as disclosure for purpose of countering unlawful employment and misappropriation of benefits (Section 31a) and disclosure for purposes of countering money laundering and terrorist financing (Section 31b).

A development that might be subsumed under the wide umbrella of administrative law are the identity infrastructures in the German eID. Secure and user-friendly identity management, including a switch from a paper-based identity card to an electronic identity card has been one of the goals of the German e-Government initiative. The introduction of the new identity card and related infrastructure has been justified by a need for a trustworthy and efficient identity management. This need is to be realized by a combination of a sovereign identity document with eID functionality for eBusiness and eGovernment that aims to provide users with a secure identity in the electronic world and afford them better protection against many types of cybercrime, such as phishing and identity theft.[352]

Proponents of the card envision that it can replace username and password, and at the same time allows services previously requiring the presence of the citizen to be provided electronically.[353] The specific design rationale is driven by a number of goals:

- Easier online authentication with more control and responsibility given to the citizen;
- Reliable authentication and high-quality data records available to the service providers;
- Data reduction and data economy through designing the eID system according to the need-to-know principle;[354]

[352] BSI (Bundesamt für Sicherheit in der Informationstechnik) (2010), *Innovations for an eID Architecture in Germany,* Bonn: BSI, p.5.
[353] Poller, A., Waldmann, U., Vowé, S. and S. Türpe. (2012) 'Electronic Identity Cards for User Authentication–Promise and Practice' 48 <https://www.researchgate.net/publication/224260803_Electronic_Identity_Cards_for_User_Authentication-Promise_and_Practice> accessed 15 March 2020.
[354] Service providers are authorized to access only data that they can demonstrate to have a real need for.

- No centralized databases of personal information;
- Privacy enhancement through the support of pseudonyms and on-card data verification;
- Protection against threats through protocol design;
- User control – entering a PIN is a requirement to grant access to any data or function.[355]

Anti-trust and consumer protection law

Are there specific articles or doctrines particular to your country in the area of competition or consumer law that are relevant for dealing with privacy and data protection in horizontal relations (e.g. antitrust cases initiated by commercial parties to break the hegemony of digital companies, blacklists for products/services in consumer relations)?

Can you explain the rationale for these provisions, e.g. by referring to the Explanatory Memorandum of the Bill introducing the provisions or to the parliamentary discussions regarding their introduction?

Indication of length: 1-2 pages A4

For a relevant development related to consumer protection see section 4.2 discussing a successful case brought by a consumer protection organization against Facebook. A similar relevant development in the field of anti-trust law is the case of the Federal Cartel Office (*Bundeskartellamt*) against Facebook and the subsequent successful appeal of Facebook to the Higher Regional Court in Düsseldorf. Instead of a separate discussion of the action of the supervisory activity and the case in front of the court, this section will offer an integrated discussion of both.

The initial case was opened by the Federal Cartel Office which in February 2019 prohibited Facebook to combine user data from different sources.[356] The background and reasoning are available in English here: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4

In its decision, the Federal Office introduced a significant restriction to Facebook's use of users' data. In short:

- Facebook-owned services (WhatsApp, Instagram) can continue to collect data, but assigning them to Facebook user accounts must be subject to users' voluntary consent.
- Assigning data collected from third-party websites to Facebook user accounts must also be subject to users' voluntary consent.

Andreas Mundt, President of the Bundeskartellamt explained this: *"With regard to Facebook's future data processing policy, we are carrying out what can be seen as an internal divestiture of Facebook's data. In future, Facebook will no longer be allowed to force its users to agree to the practically unrestricted collection and assigning of non-Facebook data to their Facebook user accounts. The combination of data sources substantially contributed to the fact that Facebook was able to build a unique database for each individual user and thus to gain market power. In future, consumers can prevent Facebook from unrestrictedly collecting and using their data. The previous practice of combining all data in a Facebook user account, practically without any restriction, will now be subject to the voluntary consent given by the users. Voluntary consent means that the use of Facebook's services must not be subject to the users' consent to their data*

[355] Poller, A., Waldmann, U., Vowé, S. and S. Türpe (n 35) 51–52.
[356] 'B6-22-16.Pdf' <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4> accessed 14 March 2020.

being collected and combined in this way. If users do not consent, Facebook may not exclude them from its services and must refrain from collecting and merging data from different sources."

The Federal Office held that the extent to which Facebook collects and merges data in user accounts constitutes an abuse of a dominant position under competition law. It argues that users are not aware of the fact that "*private use of the network is subject to Facebook being able to collect an almost unlimited amount of any type of user data from third party sources, allocate these to the users' Facebook accounts and use them for numerous data processing processes*."

The Office considers Facebook's conduct to amount to exploitative abuse in detriment to the customer and impeding competition since competitors are unable to amass so much data.

The decision of the Federal Cartel Office promised to have significant consequences for Facebook's business model in Germany. However, Facebook appealed against it to the Higher Regional Court in Düsseldorf (*OLG Düsseldorf*) which in August 2019 overturned the decision.[357] (ECLI:DE:OLGD:2019:0826.KART1.19V.00)

The Düsseldorf Court did not find anti-competitive practices in Facebook's mode of operation. They argued that the assigning of third-party data did not lead to exploitation of users since the economic weakening of the user does not occur, because the data can be easily replicated and made available to Facebook's competitors, and unlike the Cartel Office, the Court did not find the 'all-or-nothing' consent to be involuntary, since the user can weigh the advantages of using the free service against the consequences of Facebook's use of third party data. The Court also dismissed the Cartel Office's assertion that the users have difficulty understanding what data are being collected and what happens to it. In the Court's opinion, it is not a reflection of market power of Facebook, if the user does not properly read the terms and conditions. The Court also didn't agree that competitors are excluded due to the third party data assigning. The decision of the Düsseldorf Court is not final and the appeal will be decided by the Federal Court of Justice (*Bundesgerichtshof*).

Case law

See *supra* Section 4.2 for more on: Higher Regional Court in Berlin (*Kammergericht Berlin, 5. Zivilsenat*), Decision from 20.12.2019 - 5 U 9/18, ECLI:DE:KG:2019:1220.5U9.18.0A.

See *supra* Section 5.2 for more on: Higher Regional Court in Düsseldorf from 26 August 2019, VI-Kart 1/19 (V), ECLI:DE:OLGD:2019:0826.KART1.19V.00.

[357] *OLG Düsseldorf, 2682019 - VI-Kart 1/19 (V) - Verarbeitung von Nutzerdaten durch Facebook* [2019] OLG Düsseldorf VI-Kart 1/19 (V), 2019 MMR 742.

Criminal law

Relevant articles and rationale

Please provide an overview of articles in your criminal law that deal with privacy violations in horizontal relations (e.g. defamation, eavesdropping, revenge porn). Please use the table below. If any criminal acts are missing, please add them.

Criminal act	Relevant article(s)	Description
Defamation, slander and libel	§186 StGB Malicious gossip	Assertion or dissemination of untrue facts degrading or negatively affecting reputation.
	§187 StGB Defamation	Knowing assertion or dissemination of untrue facts degrading or negatively affecting reputation or creditworthiness
	§188 StGB Malicious gossip or Defamation in relation to persons in political life	
Surreptitious monitoring (visual, aural, electronic) (e.g. camera surveillance, eavesdropping, spyware)	§201 StGB Violation of privacy of spoken word	Recording privately spoken words, using a listening device to intercept privately spoken words, making available to third parties of such recording, or publicly communicating the content of private words recorded or intercepted in this way.
	§201a StGB Violation of intimate privacy by taking photographs and other images	Taking unauthorized images of people in homes or rooms protected from view, taking images of helpless people, using such images or making them available to third party.
	§202 Violation of privacy of letters	Unauthorised opening of sealed letters or papers, or learning their content without opening by technical means

	§202a StGB Data espionage	Unauthorised access to data not intended for the perpetrator that is protected from view by overcoming access protection
Harassment	§184i Sexual harassment Other forms of harassment penalized as Stalking, if they are persistent (see below)	Touching a person in a sexual manner and thereby harassing them
Location tracking	Not specifically criminalized, persistent location tracking could fall under Stalking (see below)	
Stalking	§238 StGB Stalking	Stalking another person in a way seriously restricting their lifestyle by persistently: seeking their proximity, trying to establish contacts, improperly using their personal data, threatening them or their close persons, and other similar acts.
Extortion (e.g. sextortion)	§240 StGB Coercion §253 StGB Extortion	Coercing someone to do, suffer or refrain from an act by force or threat of serious harm Coercing someone to do, suffer or refrain from an act by force or threat of serious harm (for purpose of personal enrichment)
Publication of sexual images (e.g. revenge porn)	Not explicitly, but falls under §201a(2) Additionally under §201a(3)	Unauthorised making accessible to third parties images which are likely to cause considerable damage to the image of the person depicted Making accessible to other people images of a naked person younger than 18

Publication of pictures of helpless people (e.g. filming traffic incidents)	§201a(1)(2-4)	Creating, making available to others or using images showing the helplessness of another person
Other, namely:	§202d StGB Handling stolen data	Procuring or supplying access to data which are not publicly accessible and were obtained by an unlawful act for personal enrichment or to harm another person
	§203 StGB Violation of private secrets	Unlawful disclosing of private secrets by a person who obtained them in the course of their profession (doctor, lawyer, therapist, etc.)
	§204 StGB Expoitation of private secrets	Exploitation of secrets which the perpetrator is obliged to keep secret
	§123 StGB Breach of home peace	Unauthorised entering or remaining in a dwelling, business premises or a fenced-off property

German criminal law contains a comparatively very elaborate and well-developed protection of visual privacy in section 201a of the Criminal Code. For this reason, particular focus will be given here to this provision, which is included in the Chapter 15 of the Criminal Code entitled Violations of personal life and private secrets, along with criminal offences breaching privacy of written and spoken word, data espionage, violations of secrets, among others.

The legal good protected by the provision in section 201a of the Criminal Code (protecting visual privacy) is the highly personal area of life. This includes the core content of the general personality right, including the intimate and sexual sphere, illness and death,[358] and in part also religion. Some authors express concern that the freedom of information and expression might become too restricted, if the protected area is interpreted more broadly.[359] The adoption of Section 201a and its later extensions fulfills a long-standing demand for strengthening criminal law protection of personality rights.[360] It is necessary due to the technical development of visual recording devices of the last few years, such as mobile phone and spycams, and dissemination on the internet, which made a wider range of possible attacks on privacy possible.[361]

The offence is committed in a number of alternative ways. The first alternative protects people from unauthorised making of images in the protected area of the dwelling and in rooms which are protected

[358] Kühl, 'StGB § 201a Verletzung Des Höchstpersönlichen Lebensbereichs Durch Bildaufnahmen' in Lackner and Kühl (eds), *StGB* (29th edn, 2018) 1.
[359] ibid.
[360] Heuchemer, 'StGB § 201a Verletzung Des Höchstpersönlichen Lebensbereichs Durch Bildaufnahmen' in v Heintschel-Heinegg (ed), *BeckOK StGB* (45th edn, 2020) 4.
[361] Bundestag Drucksache 15/2466, p. 5.

from view.[362] Dwelling, as the core protected area is protected as a highly personal retreat. Here, it is not a matter of property rights or ownership, so guests in other people's apartments or hotel rooms are also protected.[363] Spaces protected from view include areas such as toilets, locker rooms or medical treatment rooms. In some circumstances a garden surrounded by an opaque fence can also fulfill this function, but only if it is completely restricted from view, so if for instance it is visible from the second floor of the neighbor's house, it would not be protected. Places protected from view, but freely accessible to other people, such as sauna's in public pools, do not fulfill this function either.[364]

Individuals are protected in these spaces only to the extent concerning their highly personal area of life. The intention to violate this area is not enough, the violation must really occur.[365] The highly personal area would mostly cover nudity, details of sexual life, disease, death and the inner world of thoughts, as long as it is manifested in external appearances.[366]

Creating the image means the production of the recording of the image with technical means including the storage of the image on a data carrier.[367] Mere observation (e.g. peeping Tom), which does not permanently capture the image is not criminalised, even when technical devices such as binoculars or night vision are used,[368] since the specific harm of the offence is the pictorial perpetuation of the transitory appearance of a person.[369] The offence does, however, cover real-time transmissions of visual image by means of webcams or spycams in which an intermediate storage, but not permanent fixation occur.[370]

Germany also introduced an additional offence in the 2014 reform of the provision, covering the unlawful creation or transmission of "pictures that showcase another person's helplessness, and thereby violat[ing] their intimate privacy". The concept of 'helplesness' (*Hilflosigkeit*), as a dignity-based boundary marker of visually recording people which supplemented the earlier place/space-based boundary. Generally, *Hilflosigkeit* has two different meanings: helplessness as a subjective feeling and helplessness as an objective state of being.

The original bill spoke of images capable of inflicting considerable damage to someone's reputation or that show the person unclothed,[371] as with persons in embarrassing, degrading or unclothed situations, there is a likely interest in the picture not being made or transmitted to other parties.[372] During the legislative process, the provision was restructured: protection against making images capable of harming reputation was moved and limited to dissemination of such images (§201a(2)), and the protection against making of photographs showing someone unclothed were also limited to dissemination and to under-age victims (§201a(3)). A provision protecting against making of images showing "the helplessness of another person" was inserted in §201a(1)(2).

---

[362] Heuchemer (n 42) 11–12.
[363] Bundestag Drucksache 15/2466, p. 5.
[364] Heuchemer (n 42) 12.
[365] OLG Koblenz Resolution v 11.11.2008 - 1 Ws 535/08 = NStZ 2009 , 268, 269.
[366] Heuchemer (n 42) 14.
[367] Kühl (n 40) 4.
[368] Graf, 'StGB § 201a Verletzung Des Höchstpersönlichen Lebensbereichs Durch Bildaufnahmen', *Münchener Kommentar zum StGB* (3rd edn, 2017) 15.
[369] Kühl (n 40) 4.
[370] ibid 5.
[371] Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz, Entwurf eines ... Gesetzes zur Änderung des Strafgesetzbuches – Umsetzung europäischer Vorgaben zum Sexualstrafrecht, available at: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Gesetz-Aenderung-StGB-Umsetzung-europaeischer-Vorgaben-zum-Sexualstrafrecht.pdf?__blob=publicationFile&v=5, p. 14.
[372] Ibid., 48-49.

Examples of helplessness include victims of traffic accidents,[373] victims of violence lying bloodied on the ground, drunken people returning home,[374] and drunken teenagers.[375] People can suffer harm from such pictures, and they depict situations that the person could not control. Protection is considered especially important if it concerns situations that the persons did not cause through their own fault,[376] although the examples of drunkenness indicate that also self-caused helplessness can trigger protection. Sleep or old age by itself do not create helplessness. The duration of helplessness or the reason for it (e.g. self-induced helplessness) are not relevant.[377] The emphasis, thus, seems to be on situations outside the depicted person's control. In that sense, also §201a(2) German CC might be understood as protecting people from harmful acts they cannot really control, namely others disseminating pictures of them that can seriously harm their reputation. For further clarification of the helplessness provision see *infra* section 6.2.
Section 201a(1:3) further criminalizes use or dissemination of images made by one of the two alternatives mentioned above. Use means any use, including storing, recording, copying. A new form of criminalization in Section 201a(1:4) extends the offence to dissemination of pictures that were not unlawfully created (e.g., because there was consent, or absence of criminal intent), but made in the manner indicated in the description, e.g. by family members within the home, holiday pictures or otherwise justified recordings. The technical development has shown that the dissemination of such recordings results in new forms of crime of such as Internet stalking or Internet bullying.[378]

The criminalization of privacy-infringing recordings of people in helpless situations seems a good starting point for updating other legal frameworks in the era of social media and ubiquitous mobile cameras.

The third type of the offense, limited to dissemination, criminalises sharing of images harmful to a person's reputation. The aim of this regulation was to tackle ever more widespread cyberbullying, especially via the internet which often targets children and adolescents with serious consequences for the affected.[379] The means of obtaining such images are not relevant, and even unauthorized sharing of images which were created with permission of the victim is criminalized.[380] It may often be difficult to assess what images are suitable to significantly damage the reputation of the victim. The more inferior, embarrassing, disgusting or repulsive the respective picture appears, the easier it is to determine its suitability for damage to reputation.[381] But, if the image shows prominent people who themselves often pose pictures of themselves in questionable situations, or if an artistic purpose is asserted, the assessment becomes more difficult.[382]

Importantly, there is an exception from criminalization of the acts penalized in Section 201a. Penalties shall not apply to acts carried out in the exercise of predominantly legitimate interests, in particular art or science, research or teaching, the reporting of events or history or similar purposes. This exception, however, does not cover images made in the dwelling or spaces protected from view, demonstrating Germany's strong

[373] Bundesrat, Stenografischer Bericht, 929. Sitzung, 19 December 2014, 25.
[374] Bundestag, Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss), Drucksache 18/3202 (neu), 18. Wahlperiode, 12 November 2014, 28.
[375] Bundestag, Stenografischer Bericht, 67. Sitzung, 14 November 2014, 12.
[376] Bundestag Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss), Drucksache 18/3202 (neu), 18. Wahlperiode, 12 November 2014, 28.
[377] Kühl, K., Heger, M. (2014) Strafgesetzbuch: Kommentar, Beck-Online, StGB §243, Rn. 21.
[378] Heuchemer (n 42) 20.
[379] BT-Drs. 18/2601, 37.
[380] Graf (n 50) 70.
[381] *Fischer, '*§ 201a*', Strafgesetzbuch: StGB (64th edn, 2017)* 23.
[382] Graf (n 50) 72.

protection of the privacy of home life..[383] Also according to Section 205, the offences in 201a are only prosecuted upon request of the victim or the relatives of the victim in case the victim dies.

German law also criminalises the interceptions of "privately spoken words not intended for the perpetrator's attention" in section 201 of the Criminal Code.[384] The provision covers the interceptions of "privately spoken words,"[385] which includes all acoustically perceptible expressions of ideas. The expression need not be made consciously, even utterances made in sleep qualify. However, sounds like yawns or sighs do not, since they are not considered expressions of ideas.[386] It prohibits using an unlawfully obtained audio recording or making such a recording available to a third party, as well as publicly communicating (either verbatim or the essential content of) the privately spoken words of another that were overheard or recorded in violation of the relevant eavesdropping provisions. The provision dates back to the 1960 amendment draft of the Criminal Code[387] It serves the constitutionally guaranteed free development of personality by ensuring the confidentiality of oral statement, following the idea that what was meant as a fleeting expression of life should not be transformed into an always reproducible form.[388]

The criminalization of Stalking is also worth mentioning as a potential gap-filler in criminalization. Due to the open-ended definition, it can potentially cover a wider range of high intensity privacy intrusions which may not be criminalized separately. The criminal offense of stalking is construed by three main elements: (1) long-term, persistent conduct, (2) which is harassing, defined by a non-exhaustive list, including seeking proximity of the victim, trying to establish contact, abusing personal data of the victim, threatening the victim with harm and other similar acts, (3) and which causes a certain effect, namely that the victim's lifestyle is severely affected (this effect has to actually occur). Stalking may, therefore, cover various privacy intrusive behaviour, which is persistent and causes fear, distress and results in changing habits of the victim. Thus, the criminalization of stalking mainly protects the privacy of the mind and behavioural privacy, the victim's freedom to act and make decisions.[389]

Case law

Since the provision protecting people from being filmed or photographed in a way that shows their helplessness is relatively new, the case law in rather limited. However, a case has reached the Supreme Court that made an important clarification about how the provision is to be interpreted. Helplessness refers to image content and not just the circumstances of its creation: helplessness must be visible in the image. In a case where a perpetrator used his cell phone to video-record an abducted man who, under threat of violence, inserted a bottle into his rectum, the German Federal Supreme Court (*Bundesgerichtshof*) determined that the recording would only "show helplessness" if the context of the threat was also evident in the recording. Showing the act of inserting the bottle rectally, in itself, does not sufficiently show helplessness.[390] The emphasis, thus, seems to be on situations where people are portrayed in a situation they do not control. In that sense, § 201a(2) German CC protects people not so much against acts against their autonomy (in the sense that, being helpless, they cannot prevent pictures being made), but against

[383] Section 201a(4) StGB.
[384] Section 201(1)(2) StGB.
[385] Section 201(1)(2) StGB.
[386] Heuchemer, 'StGB § 201 Verletzung Der Vertraulichkeit Des Wortes' in v Heintschel-Heinegg (ed), *BeckOK StGB* (45th edn, 2020) 3.
[387] Graf, 'StGB § 201 Verletzung Der Vertraulichkeit Des Wortes', *Münchener Kommentar zum StGB* (3rd edn, 2017) 6.
[388] ibid 2.
[389] Gericke, 'StGB § 238 Nachstellung', *Münchener Kommentar zum StGB* (3rd edn, 2017) 1.
[390] BGH, judgement of 25 April 2017, 4 StR 244/16. ECLI:DE:BGH:2017:250417B4STR244.16.0.

acts that showcase their lack of autonomy. Such acts fundamentally undermine the possibility of impression management, since they take away someone's image as having agency. Especially for people in embarrassing or degrading situations, there is an interest in pictures not being transmitted to other parties.

Actions by the public prosecution, police or supervisory authorities

According to the Ministry of Justice, the criterion for whether an image is suitable to significantly damage the image of the person depicted (as criminalised in section 201a(2) of the Criminal Code) is the assessment by an average viewer.[391]

Significance in practice

Although the provisions protecting visual privacy of people are (in large part) rather recent (and therefore it is somewhat difficult to judge their significance in practice), already a new extension is being proposed and in the legislative process, which would extend the special protection to (deceased) victims of road accidents and would also cover the phenomenon of up-skirting.[392] Since this is the second reform of section 201a in the last few years, it shows that criminalization is seen as a useful and effective tool in this sphere. On the other hand, the piecemeal introduction of new forms of criminalization shows that there is still a need for finetuning the provisions, or that perhaps instead of a more general regulation covering possible future developments, the legislature simply reacts to problems arising as they arise. A proposal for extending the draft by also criminalizing the undesired filming of female breasts (cleavage) further shows this approach.[393] This legislative approach is criticized in literature.[394]

Civil and commercial law

Relevant articles and rationale

In German Civil Code (BGB), main Tort law provisions relevant for horizontal privacy seem to be Section 823 (Liability in damages) and Section 824 (Endangering credit). Under Section 823, anyone who unlawfully (with fault) injures the life, body, health, freedom, property or another right of another person is liable to make compensation for damages arising from this. The same duty is held b a person who commits a breach of statute that is intended to protect another person. The purpose of this section is to sanction of illegal violations of human relationships which form the basis of community life. It is based on the general principle *neminem laedere*.[395] The goal is on one hand to compensate damages to the injured party[396] and at the same time the general prevention which is of particular importance in the event of violations of the general personality right.[397] The damages include the compensation of pain and suffering, not only material damage, otherwise the injured party would be defenceless in connection to many aspects of general personality rights.[398]

[391] Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz, Entwurf eines ... Gesetzes zur Änderung des Strafgesetzbuches – Umsetzung europäischer Vorgaben zum Sexualstrafrecht, 48-49.
[392] Akad Steven Bonnin and Sebastian Berndt, 'Rechtsdogmatische Überlegungen Zum Phänomen Des Upskirting – Zugleich Eine Kritische Betrachtung Aktueller Entwicklungen' [2020] Neue Juristische Online-Zeitschrift 129, 129.
[393] Tonio Walter, 'Walter: Kleines Beispiel, Große Fragen' [2020] Zeitschrift für Rechtspolitik 16, 16.
[394] ibid 18; Bonnin and Berndt (n 65) 131.
[395] Förster, 'BGB § 823 Schadensersatzpflicht' in Bamberger and others (eds), *BeckOK BGB* (53rd edn, 2020) 1.
[396] ibid 7.
[397] ibid 9.
[398] ibid 13.

Under Section 824 BGB, a person who untruthfully states or disseminates a fact that is qualified to endanger the credit of another person or to cause other disadvantages to their livelihood must compensate them for damages, if this person knew or should have known about the untruthfulness. If the person is unaware of the untruthfulness and has a justified interest in the communication, is not obliged to pay damages. Unlike Section 823, the damages here do not include the pain and suffering, since the provisions purpose is to protect the financial interest of the injured party. Aspect of the general personality right, such as honour are thus only protected indirectly, in so far as it impacts the creditworthiness.[399] The provision equally applies to statements made on internet platforms, but does not generally provide legal basis to claim damages from the intermediaries who provide the technical infrastructure, only to the person who made the incriminating statement.[400]

More specific provisions relevant to horizontal privacy in the field of civil law can be found in the Law on Copyright in the Works of Fine Arts and Photography (KUG: Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie), in particular Section 22 which establishes portrait rights and Section 23 which provides some exceptions to this right. Under Section 22 KUG, images may only be distributed or publicly displayed with the consent of the person depicted (consent is assumed, if the person received renumeration for having been reproduced). The portrait rights are passed on to relatives after death for a period of 10 years. It creates a right to a person's own image, an intellectual property right which is not the author's, but only the person's who is depicted, who can decide whether and how it is presented in public.[401] The provision is supposed to preserve the right to self-determination regarding the visual representation of a person.[402]

Section 23 KUG establishes some exceptions from the above. Images may be disseminated and displayed without consent, if they are portraits from the field of contemporary history, images in which people only appear as accessories alongside a landscape or other location, pictures of gatherings in which the people depicted have participated and portraits that are made to order, if the displaying serves a greater interest in art. However, the authority to distribute and display under these exceptions does not apply, if it would violate a legitimate interest of the person depicted. Connecting interestingly to the Criminal law discussion of protecting helpless peoples' visual privacy (see *supra* Sections 6.1 and 6.2), the concept of helplessness has been discussed in relation to artistic street photographs and the limits placed around artistic freedom to photograph people (§23 KUG). In this context, making of street photographs showing death or dying of people is not allowed as it is a deep intrusion into the intimate sphere. Helplessness is listed with concepts such as illness, distress, emotional outburst as situations where the right to artistic expression of the photographer needs to be balanced against personality rights of the photographed person[403] as no one shall be photographed in a way that deprives them of their dignity.[404]

Intermediary liability and duty of care for information society services

The German Telemedia Act (TMG: *Telemediengesetz*) which transposes the e-Commerce Directive, generally provides a framework of intermediary liability equivalent to Art. 12-15 of the Directive. Service

[399] Wagner, 'BGB § 824 Kreditgefährdung', *Münchener Kommentar zum BGB* (7th edn, 2017) 3.
[400] ibid 9.
[401] Engels, 'KunstUrhG § 22 [Recht Am Eigenen Bilde]' in Ahlberg and Götting (eds), *BeckOK Urheberrecht* (26th edn, 2019) 2.
[402] ibid 5.
[403] Angela Hildebrand, 'Abbildungen von Personen Bei Künstlerischer Street Photography' [2016] ZUM 305, 313.
[404] ibid 310.

providers are responsible for the content they themselves make available for use (content providers[405]), but are not obliged to monitor the information transmitted or stored by them or to search circumstances that indicate illegal activity, although they are still obliged to remove or block content according to general laws due to judicial or official orders (Section 7 TMG). Generally, the responsibility of the service provider shall increase the closer to the content in question the service provider is.[406] Providers providing transmission are not responsible, unless they initiate the transmission, select the addressee of the transmission, or selected or changed the transmitted content (Section 8 TMG). Providers are also not responsible for automatic, temporary storage which serves the purpose of making the transmission to other users, unless they change the information, and they observe the conditions for access to the information, comply with industry standards. They have to act immediately to remove or block access to content as soon as it becomes aware that the content was removed from the network at the point of origin of the transmission or when ordered by a court or an administrative authority (Section 9 TMG). Host providers are not responsible for content as long as they have no knowledge of the illegal act or the information and, in the event of claims for damages, they are also not aware of any facts or circumstances from which the illegal act or the information becomes obvious, or they act immediately to remove the information or block access to it as soon as they became aware of it (Section 10 TMG). The knowledge referred to in Section 10 must be concrete knowledge including the location of the illegal content. Simply knowing that there is illegal content somewhere in storage is not enough to establish liability.[407] The removing or blocking must also be technically and reasonably possible, the reasonableness being weighed up to the interests of the injured and the general public on one side and the interests of the provider on the other.[408]

Relevant to mention in this section are also the duties established under the Network Enforcement Act (*Netzwerkdurchsetzungsgesetz*). These have been discussed in detail elsewhere (see *supra* Section 3 of this report).

Regulation of distribution and sales of goods and services

Requirements in technology

German privacy laws and their interpretation result in some technologies being more limited in use in Germany than elsewhere. For instance, Section 4 of the German Data Protection Act (*Bundesdatenschutzgesetz*) bans continuous recording of public spaces (see *supra* Section 4.1). As a result, it is not allowed to operate dashcams that would continuously record the traffic on the road. However, the Federal Court of Justice has accepted dashcam footage as evidence, stating that for obtaining such footage, continuous recording is not necessary. The recording can also be set up in such a way that it continuously overwrites itself and only relevant footage (e.g. of an accident) is saved.[409] Another example

[405] 'BeckOK StGB | Providerhaftung Rn. 15-30 - Beck-Online' <https://beck-online.beck.de/?vpath=bibdata%2fkomm%2fBeckOKStGB_45%2fcont%2fBECKOKSTGB%2ePROVIDERHAFTUNG%2eglD%2ehtm> accessed 15 March 2020.
[406] ibid 15.
[407] 'BeckOK StGB | Providerhaftung Rn. 22-25 - Beck-Online' 23 <https://beck-online.beck.de/?vpath=bibdata/komm/BeckOKStGB_45/cont/BECKOKSTGB.PROVIDERHAFTUNG.glD.glII.htm> accessed 15 March 2020.
[408] ibid 25.
[409] 'BGH, Urteil Vom 15.05.2018 - VI ZR 233/17 - OpenJur' <https://openjur.de/u/2121277.html> accessed 16 March 2020.

dates back to 2010 when German authorities required that Google Street View lets Germans to request that their house is blurred in the service.[410]

Case law

Caroline von Monaco III, Federal Constitutional Court, Order of the First Senate of 26 February 2008 - 1 BvR 1602/07, ECLI:DE:BVerfG:2008:rs20080226.1bvr160207

In the German proceedings of the well-known Von Hannover v. Germany case at the ECtHR, the Federal Constitutional Court made a number of interesting observations in relation to the right to one's image. The case related to pieces of photojournalism of the family of Prince Rainier of Monaco, in which their everyday life was depicted. (in a part of the case) The lower courts in Germany authorized the publication of the photographs. The Constitutional Court found this in part to be touching upon the personality rights, in its aspect of safeguarding one's own image.[411] The right to one's own image grants the individual a means of influencing the creation and use of pictorial recordings of their person. The need for protection arises from the possibility to remove an image from its context and be reproduced in other circumstances which the person concerned cannot control. The easier this is, the more protection is needed. Greater endangerment of personality comes with advancements in recording technology, such as cameras built in mobile phones, small and portable cameras, which expose prominent people to be photographed in all situations without warning and their knowledge, to be published in the media. The covert approach of the photographer brings a particular need for protection, especially if the content of the recording relates to everyday like, relaxing, during which the person does not expect to be photographed.[412]

Actions by a governmental agency

Supervisory action related to the Network Enforcement Act (see *supra* Section 3):

In July 2019, the Federal Office of Justice (*Bundesamt für Justiz*) issues a fine in the amount of 2 million Euros against Facebook for violating the Network Enforcement Act. The violation was found in the way Facebook published its transparency report for the first half og 2018. Facebook provided incomplete information in its report on the number of complaints received about unlawful content under the Act. The report listed only a fraction of the complaints filed by users. Facebook offered the users two channels to issue complaints - its own standard channels and the Network Enforcement Act channels. Users were steered towards the standard channels and the Network Enforcement Act channels availability was not transparent. This led to only a fraction of actual compaints being reported under the Network Enforcement Ac, which affected the degree to which meaningful information has been provided on the measures taken in response to the complaints. Additionally, the Federal Office of Justice found that Facebook innacurately reported on measures to inform complainants and users, especially whether this information includes the grounds for the decision taken on the reported content.[413]

Part 3: Mechanisms other than legislation

[410] 'Wie widerspreche ich?' (*stern.de*, 11 August 2010) <https://www.stern.de/digital/online/google-street-view-wie-widerspreche-ich--3110486.html> accessed 16 March 2020.
[411] *Caroline von Monaco III*, Federal Constitutional Court, Order of the First Senate of 26 February 2008 - 1 BvR 1602/07, 45.
[412] Ibid 46.
[413] 'BfJ - Startseite - Federal Office of Justice Issues Fine against Facebook' <https://www.bundesjustizamt.de/DE/Presse/Archiv/2019/20190702_EN.html;jsessionid=B1B7EDD9E3D423AFBC70795510712ED3.1_cid392?nn=3449818> accessed 16 March 2020.

In this part we want to explore mechanisms outside of the legislation described in the previous part that are applied in your country to regulate privacy and data protection in horizontal relations.

Non-legal mechanisms

Awareness

There are indications that the German people on average put a high value on privacy compared to other nations. To illustrate, according to research presented by the Harvard Business Review, the average German is willing to pay significantly more to protect their personal data than the average Brit, American or Chinese citizen.[414] Another example is the notorious German preference for cash payment over electronic payment, indicating a preference for privacy over efficiency. In 2017, three quarters of all purchase transactions in Germany were in cash.[415] To compare, in the Netherlands, in 2016 only forty five percent of transactions were in cash.[416] Another example is the limited success of the Google Street View service in Germany. When Google announced its plans to map the street of Germany's big cities at the beginning of last decade, it sparked outrage among Germans.[417] The German Consumer Protection Minister called the efforts of google a "comprehensive photo offensive (that) is nothing less than a million-fold violation of the private sphere".[418] The coverage of Google Street View remains limited in Germany compared to other European Countries. The German attitude towards privacy illustrated by these examples is often attributed to their experience of two authoritarian regimes - the Third Reich and the DDR - and the unwillingness to repeat these experiences.

[414] Timothy Morey, Theodore "Theo" Forbath and Allison Schoop, 'Customer Data: Designing for Transparency and Trust' [2015] *Harvard Business Review* <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust> accessed 16 March 2020.
[415] Heike Mai and others, 'Cash, Electronic or Online: How Do Germans Pay?' 6.
[416] 'From Cash to Cards_tcm46-372117.Pdf' <https://www.dnb.nl/binaries/From%20cash%20to%20cards_tcm46-372117.pdf> accessed 16 March 2020.
[417] Claire Cain Miller and Kevin J O'Brien, 'Germany's Complicated Relationship With Google Street View' (*Bits Blog*, 23 April 2013) <https://bits.blogs.nytimes.com/2013/04/23/germanys-complicated-relationship-with-google-street-view/> accessed 16 March 2020.
[418] DER SPIEGEL, '"Million-Fold Violation of the Private Sphere": German Minister Takes on Google Street View - DER SPIEGEL - International' <https://www.spiegel.de/international/germany/million-fold-violation-of-the-private-sphere-german-minister-takes-on-google-street-view-a-676616.html> accessed 16 March 2020.

16.4 Bijlage 4: Landenrapport Polen

Auteur: Ivan Skorvanek

Part 1: Introduction

Legal system

Poland is a Civil law jurisdiction and a unitary state. The formal sources of law are the constitution, the statutes and the ratified international agreements. Major field of law are codified. In this, and many other aspects, Polish legal culture looks for inspiration to the large civil law legal systems, in particular the German legal system. Due to the significant and rapid societal changes in the last 31 years (since the fall of communism), Polish legal order also underwent significant reforms, in particular to strengthen democratic institutions and the rule of law (and recently drawn criticism and EU proceedings from backtracking in these fields), to adapt to a market economy and to join the European Union. For these reasons, the Polish legal order may not be as mature as western European legal orders, nor does it come up with as many original and innovative solutions (focus has been on catching up, not leading the way). The legal culture is strongly formalistic, focusing on written laws and preferring literal interpretation. Some authors consider this strong formalism and positivism typical to the post-communist countries to be a heritage of the authoritarian regimes - the legal professionals confronted by the disregard of the former regime for their own laws, developed a defensive mechanism in which they placed legality and legal certainty above any other values (and later those seeking to excuse their own actions during the one-party system found solace in the justification 'the law is the law').[419]

Fundamental rights framework

Horizontal effect of constitutional law

The notion that the Constitution governs not only the relations between the state and citizens, but also some horizontal relations between private parties is widely accepted in Polish doctrine.[420] Basic rights in Poland all find their basis in the protection of human dignity. Art. 30 of the Constitution states that the natural and inalienable human dignity is the source of freedoms and rights of a person and a citizen. It is inviolable and its respect and protection is the duty of the government. The duty to protect human dignity, therefore, creates a positive obligation on the part of the state not only to respect human dignity and rights arising from it, but to also protect them from violations by others. The positive obligation of the state to protect private life of citizens from interferences of others has been confirmed by the Constitutional Court.[421] Furthermore, Art. 31 of the Constitution states that everyone is obliged to respect the freedoms and rights of others. In this way, the constitutional text establishes a horizontal duty to respect basic rights for everyone.[422] This, however, is largely declaratory, since there is no direct legal remedy against violations of constitutional rights by private parties. It is the responsibility of the state to create statutes and other

[419] Kateřina Šimáčková, 'Fiktívní, Nebo Reálná Ústava' in Bobek, Molek and Šimíček, *Komunistické právo v Československu* (Mezinárodní politologický ústav 2009) 142–143.
[420] Anna Młynarska-Sobaczewska and others (eds), *Horyzontalne oddziaływanie Konstytucji Rzeczypospolitej Polskiej oraz Konwencji o ochronie praw człowieka i podstawowych wolności* (Biuro Trybunału Konstytucyjnego 2015) 25.
[421] Decision of the Constitutional Court *from 11 October 2011,* K 16/10.
[422] Młynarska-Sobaczewska and others (n 3) 122.

normative acts that offer sufficient protection of constitutional rights (for instance in criminal law, or the personality rights in civil law). Everyone who's rights were violated has a right under Art. 79 of the Constitution (after using other available remedies) to file a constitutional complaint to the Constitutional Court about the compatibility of a lower-level law on the basis of which the lower courts decided with the constitution. Therefore, according to the literature the horizontal effect of constitutional norms is actually a 'mental shortcut' under which the scope of application of constitutional norms regarding freedoms and rights in private law relations is hidden.[423]

Personality rights and fundamental rights protection

Personal rights (or more precisely personal goods) are a category closely connected to private law and listed in Art. 23 of the Civil Code: health, liberty, honour, freedom of conscience, name or pseudonym, inviolability of the home, scientific and artistic creation, etc. (for more see *infra* Section 7) It is an open list of immaterial personal goods belonging to the subject of civil law, which are considered important in the society and deserving protection of the law.[424] These personal goods protected by private law find their source in the fundamental rights protected in the constitution. As mentioned above, human dignity is the basis of all rights. In the previous (authoritarian socialist) regime, privacy was not the focus of interest (formally, only the home and communications were protected).[425] In the 90s, the Supreme Court confirmed the existence of the right to privacy on the basis of the civil law system protecting personal goods.[426] A more systematic and wide-ranging protection o privacy was brought by the new Constitution in 1997,[427] which protects the constituting elements of privacy in Art. 47-50: private and family life, honour, good name, decisional privacy (Art. 47), parental rights (Art. 48), secrecy of communications (Art. 49), the inviolability of home (Art. 50). Data protection find its constitutional basis in the protection of informational self-determination in Art. 51. This is not considered to be a constituting element of privacy, but rather an aspect of this right that overlaps (in one way or another) with all the other constituting elements listed above.[428] The right to privacy is therefore also protected in the aspect of personal data[429] which guarantees a person a certain state of independence with which the individual can decide the scope and the range of sharing information about one's life with others.[430] In relation to privacy, a distinction is made between an intimate sphere and personal sphere, the latter being more open to interference.[431]
Banaszewska (based on the Polish Constitution) identifies the following goods associated with the right to protection of private life:

- Personal rights of human beings
- Integrity of a human being
- Right to honour
- Right to one's image and voice
- Secrecy of correspondence
- Inviolability of the dwelling

[423] ibid 30.
[424] Chałubińska-Jentkiewicz and Karpiuk, *Prawo Nowych Technologii - Wybrane Zagadnienia* (Wolters Kluwer) 324.
[425] Radosław Koper, *Jawność Rozprawy Głównej a Ochrona Prawa Do Prywatności w Procesie Karnym* (Wolters Kluwer 2010) 98.
[426] Supreme Court Decision, 8 April 1994, III ARN 18/94.
[427] Andrzej Sakowicz, *Prawnokarne Gwarancje Prywatności* (Wolters Kluwer 2006) 96.
[428] Koper (n 9) 133–134.
[429] Constitutional Court Decision, 19 May 1998, U 5/97.
[430] Constitutional Court Decision, 23 February 2010, K 1/08.
[431] Marcin Pryciak, 'Prawo do prywatności' 19, 221.

- Protection of personal data and data relating to property (financial situation)
- Intimate sphere
- Family life and social life[432]

Extra legem, intra ius

I am not aware of this. Polish legal culture is rather formalistic and relying on statutory or other written law. The role of jurisprudence is more in clarification and interpretation of written principles (see below Section 2.4).

Relevant case law (national)

The Constitutional Court, in its various decisions created the classification of guarantees of the right to privacy. The first sphere protected through the right to privacy is the informational autonomy in relation to, e.g.:

- Health situation (Decision from 19 May 1998, U 5/97; Decision from 19 February 2002, U 3/01);
- Economic situation (Decision from 20 November 2002, K 41/02);
- Family status (Decision from 13 July 2004, K 20/03);
- Political affinity (Decision from 26 October 2005, K 31/04);
- Name and appearance (Decision from 18 July 2011, K 25/09);

The other sphere protected sphere is the decisional autonomy of the individual, in relation to e.g.:

- Decisions about one's life and health (Decision from 11 October 2011, K 16/10);
- Decisions about family life (Decision from 28 April 2003, K 18/02);
- Decisions about children's upbringing (Decision from 2 December 2009, U 10/07);

Together, these decisions create a framework of the personal goods protected under the umbrella of privacy rights protected in Art. 47-51 of the Constitution.

The role of providers and distributors

-

Part 2: Protection of privacy and data in horizontal relations

Data protection legislation

Relevant articles and rationale

The Polish legislator's use of the opening clauses in the GDPR has been relatively limited. Most the of deviations are of no particular importance for this report. Worth mentioning is the published list of processing activities by the Polish supervisory authority of processing activities for which a DPIA will be required. These include evaluation, including profiling and prediction for purposes that may negatively impact the legal, physical, financial or other status of a person, automated decision-making that produces such results and processing of special categories of personal data (concerning convictions).[433]

[432] Anna Banaszewska (2013), 'Prawo do prywatności we współczesnym świecie', Białostockie Studia Prawnicze, 13, 127-136.

[433] Full list available here: https://giodo.gov.pl/pl/file/13366.

Many of the specific Polish deviations from the general framework relate to the labour law field. This includes activities which according to the supervisory authority are required to have a Data Protection Impact Assessment, for example monitoring of working time and IT systems, processing of employee biometric data and employee productivity assessment systems.[434] Art. 111 of the Polish Data Protection Act (*Ustawa o ochronie danych osobowych*) also amends the provisions of labour law on employee monitoring. CCTV in the workplace is only allowed to protect property, production control and confidential information, and not allowed at all in bathrooms/toilets, changing rooms, canteens and rooms of trade unions. The recordings can be retained for 3 months and only used for the purpose specified above. Employees must be notified of such monitoring at least 2 weeks in advance.[435]

Case law

I am not aware of relevant case law relating to the new legislation. Under the previous legal regime, the courts have questioned the processing of biometric data by employers, even when the employees consented to this. This line of case law, however is no longer relevant since the Labour Code has been amended to enable collection of biometric data and specified the conditions when this is allowed.[436]

Actions by the supervisory authority

Since the coming into force of the GDPR and the new Data Protection Act, the Personal Data Protection Office imposed several fines on private companies. The largest case involved the company Morele.net which was fined 2,8 Million PLN (appr. 650 thousand Euros) for not putting in place appropriate organisational and technical measures to the risk posed by their processing, resulting in data of more than 2 million people being compromised. The data concerned included names, phone numbers, emails, addresses, personal ID numbers, the series and number of identity documents, educational background, source of income, amount of net income, cost of living, family status, credit commitments and maintenance obligations. The risk of adverse effects, such as identity theft, was deemed very high by the Personal Data Protection Office. One of the reasons for the infringement was the ineffective monitoring of potential risks, the lack of technical and operational measures and this formed the basis for the decision to issue the fine.[437]

In another case (the first fine to a private company under the new rules), the Personal Data Protection Office fined a credit information agency Bisnode Polska for failing to fulfil the information obligation resulting from Art. 14 GDPR. The amount of the fine was more than 940 thousand PLN (more than 200 thousand Euros). The company processed data regarding sole entrepreneurs gathered in other registers, containing the address and contact data of such persons. Since the exception to the information obligation for data gathered from publicly available sources does not apply to sole entrepreneurs, the company was found in breach of the GDPR.[438]

The Lower Silesian Football Association was also fined an amount of appr. 12 thousand Euros for online disclosure of sports judges personal data, which included unnecessary information such as their addresses

[434] Ibid.
[435] Art. 22^{2} of the Labour Code (Kodeks pracy).
[436] Art. 22^{1b} of the Labour Code (Kodeks pracy).
[437] 'Decyzje Prezesa UODO - UODO' <https://uodo.gov.pl/decyzje/ZSPR.421.2.2019> accessed 18 March 2020.
[438] 'Decyzje Prezesa UODO - UODO' <https://uodo.gov.pl/decyzje/ZSPR.421.3.2018> accessed 18 March 2020.

and ID numbers. Since the Association self-reported on this breach, the Personal Data Protection Office applied mitigating circumstances and lowered the fine.[439]

Administrative, anti-trust and consumer protection law

Relevant articles and rationale

A number of privacy intrusive and harassing activities which are not serious enough to trigger criminal law sanctions are covered by the Code of (administrative) offences. These are acts which do not reach the minimum seriousness required by the criminal law and are resolved in administrative proceedings, usually resulting in a fine or some form of restriction of liberty (not prison). Art. 107 covers malicious misleading or harassing of another person in order to tease them. Art. 140 covers public committing of 'unkind pranks'. Art. 141 covers the placing of obscene advertisements, inscriptions or drawings in public places, or committing verbal indecency. Furthermore, disturbing peace, public order, night rest or causing scandals in a public place by shouting, noise, alarm or other misconduct is covered by Art. 51, including hooligan behaviour and misconduct caused by alcohol consumption. Various of these laws have been used to sanction numerous forms of stalking before it was criminalised.[440]

Various sectoral laws regulate visual and other recording of people. For instance, the Act on safety of mass events, permits the organisers of mass events to record the image and the sound of such events. If such recordings can serve as evidence in criminal proceedings or administrative proceedings, they should be given without delay to the relevant authorities. Other recordings shall be kept for at least 30 days and destroyed no later than 90 days after they were created.[441] Another example is the Act on gambling which requires to install monitoring cameras in the premises where gambling takes place, so the proper application of the rules of the game can be verified. The footage can only be released to financial authorities, the police and the participants in the game, as well as judicial authorities, and is kept for three years.[442]

Anti-trust and consumer protection law

In the field of consumer protection, an interesting Polish feature is that the protection of privacy of consumers has an explicit constitutional basis. Art. 76 of the Constitution, entitled Protection of consumers stipulates that public authorities protect consumers, users and tenants from activities that threaten their health, privacy and security as well as from unfair market practices. The need for such protection stems from the fact that the consumer is in a weaker position on the market, which can lead to various breaches of their private sphere, for example by various marketing techniques or door-to-door selling.[443] However, the provision has a declaratory character, in the sense that the legal obligation it creates has an addressee, but there is no one who can enforce it, because the obligation is supposed to be clarified in lower-level laws and cannot be a subject of a constitutional complaint[444] (see *supra* Section 2.1 for more on constitutional complaints).

---

[439] 'Aktualności - UODO' <https://uodo.gov.pl/pl/138/1448> accessed 18 March 2020.
[440] Marek Mozgawa, 'Przestępstwa Stalkingu (Nękania) i Podszywania Się' in Jarosław Warylewski, *Przestępstwa przeciwko dorbom indywidualnym* (CH Beck 2012) 435.
[441] Art. 11 of the Act on safety of mass events.
[442] Art. 15b of the Act on gambling.
[443] Justyna Węgrzyn, 'Ochrona praw konsumentów i innych osób przed nieuczciwymi praktykami rynkowymi' 14, 781.
[444] ibid 783–784.

Criminal law

Relevant articles and rationale

Criminal act	Relevant article(s)	Description
Defamation, slander and libel	Art. 212 Defamation	slander of persons, groups of people, institutions, legal entities or organizational units, by attributing it such acts or attributes which can harm their reputation among the public.
	Art. 216 Insult	Whoever insults another person, even if the other person is not present, if it is done publicly or with the intention that the insult reaches the victim.
Surreptitious monitoring (visual, aural, electronic) (e.g. camera surveillance, eavesdropping, spyware)	Art. 267(3) Unlawful obtaining of information by technical means	Whoever with the aim of obtaining information to which they are not authorized uses an eavesdropping, visual or other device or program.
	Art. 191a Breach of visual privacy	Whoever records the image of a naked person or a person during sexual activity, using against her force, unlawful threat or deceit.
Harassment	Intensive forms as Stalking (see below) Sexual harassment criminalized as a form of Insult in Art. 216	
Location tracking	Possibly as stalking, if persistent	
Stalking	Art. 190a(1)	Whoever, through persistent harassment of another person or her close person gives rise to circumstances that create a justified feeling of

		insecurity or significantly violates her privacy.
Extortion (e.g. sextortion)	Art. 191(3) Extortion	(Whoever by force or unlawful threats forces another to do something) for one's own gain.
Publication of sexual images (e.g. revenge porn)	Art. 191a Breach of visual privacy	Whoever disseminates the image of a naked person or a person during sexual activity without her permission.
Publication of pictures of helpless people (e.g. filming traffic incidents)		
Other, namely:	Art. 217 Breach of physical integrity Art. 193 Breach of home peace Art. 267(1-2) Breach of secrecy of correspondence and hacking Art. 190a(2) Identity theft	Whoever hits another person or violates their bodily inviolability in another way. (protects dignity, no physical harm required) Whoever encroaches into another person's house, apartment, premises, rooms or a fenced area, or despite a request by the authorized person does not leave such place. (1) Whoever without authorization obtains access to an information not meant for them, by opening a sealed letter, connecting into a telecommunications network or by breaking or avoiding electronic, magnetic, informatics or other special protection of such network. (2) who without authorization obtains access to the whole or a part of an informational system. Whoever pretends to be someone else usign their image or other personal

		data with the aim to cause that person a financial or other harm.

Analysis of criminal law provisions

Polish Criminal Law protection is particularly strong in several aspects, not necessarily the subject matter that is protected by the scope of protection.

For instance, Art. 267 of the Criminal Code (*Kodeks Karny*) criminalises various forms of unlawful access to information - by opening letters, connecting to a telecommunications network, accessing the whole or a part of computer system (this even without overcoming security measures), by eavesdropping, visual or other tools or programs. It also criminalises revealing information obtained in way described above to another person. Particularly interesting is the wide-ranging criminalisation of access to computers and the technologically neutral criminalisation of various forms of technology-mediated surveillance.

The **unlawful access to computers** is criminalised in Art. 267(2) even if the perpetrator does not overcome protection or security measures. The leading Polish cybercrime scholar Adamski expresses concern that the insertion of this provision will extend criminalisation too far, since the law enforcement authorities are given *de facto* discretion to label minor acts as criminal offences.[445] The official reason for penalising pure access presented by the legislature was its usefulness as a legal weapon against distributors of spyware and other malicious software used for taking over control over infected computers.[446]

Another particular feature of the Polish Criminal Code is the criminalisation of **hitting another person or other violations of bodily inviolability** in Art. 217 of the Criminal Code, even if no physical harm is caused. The legal good protected by Art. 217 is honour and bodily inviolability of physical persons, and the protection of the bodily sphere of every individual. In this way, inviolability of the person, dignity, liberty and personal safety are protected.[447] If the violation is a result of a provocation of the victim, the court may decide not to penalise it. Hitting is defined as interfering with the body of the other person with a hand, other body part or even a tool such as a stick. Other means of interfering with the body include things like hair pulling choking, tripping, spitting on someone, removing glasses or a hat, pinching, throwing objects at someone, or spraying them with something. [448]

The criminalisation of offenses against **honour and reputation** is particularly extensive in Poland and potentially open to penalising rather trivial or harmless expressions. Art. 212 of the Criminal Code criminalizes slander of persons, groups of people, institutions, legal entities or organizational units. Part of the literature is of an opinion that the provision applies not only to factual statements, but also expressions of opinion.[449] The provision also applies when the slanderous statements do not originate from the perpetrator and have been expressed by someone else already or are already widespread among the public.[450] The provision appears to have a very extensive scope, and is not limited to individuals, but also legal entities. As an exception, permissible criticism is not criminalized, but it is also hard to define. Art. 213

[445] Andrzej Adamski, Opinia do projektu ustawy z druku nr 458 Rządowy projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Opinion on the bill amendment of the Penal Code for the Office of Legal Analyses of the Sejm) http://orka.sejm.gov.pl/rexdomk6.nsf/Opdodr?OpenPage&nr=458.
[446] Explanatory Memorandum of the draft amendment of the Penal Code of 28 October 2008.
[447] Joanna Długosz, 'Art. 217' in Michał Królikowski and Robert Zawłocki, *Kodeks karny. Część szczególna. Tom I. Komentarz do artykułów 117–221* (CH Beck 2013) 840–841.
[448] ibid 843.
[449] Joanna Długosz, 'Art. 212' in Michał Królikowski and Robert Zawłocki, *Kodeks karny. Część szczególna. Tom I. Komentarz do artykułów 117–221* (CH Beck 2013) 804.
[450] ibid 805.

provides another exception from criminalization, by allowing the proof of truth to be presented by the perpetrator.

Under Art. 216 of the Criminal Code, whoever insults another person, even if the other person is not present, if it is done publicly or with the intention that the insult reaches the victim, commits a criminal offence. As with slander, the offence only carries a prison sentence, if done by means of mass media. In case the insult resulted from provocative behaviour of the victim or if the victim reacts by physically attacking the perpetrator, the court may waive the punishment. The difference in comparison to slander is that it only protects natural persons. At the same time, in the case of insult, proof of truth, or proof of public interest cannot be performed, since it is irrelevant. Insult is usually committed by expressing offensive words or offensive gestures,[451] sexual harassment or general ridicule.[452]

Related to the protection of the body, but not based on bodily inviolability, is **the protection of people's image**. Polish criminal law protects the intimate image of people, that is the image of their naked body or their body during sexual activity in Art. 191a. Additionally, by criminalizing visual surveillance of people with intention to obtain information to which one is not authorized in Art. 267(3), the Criminal Code potentially extends the protection to other situations in which people have an expectation of privacy.

Art. 191a contains two separate criminal offences: **the creation of voyeuristic images and the dissemination of such images**. The first criminal offence in Art. 191a, creation of images, protects a legal good that is an emanation of the freedom from force, threat or deceitful action in deciding how and if at all one's intimate image is to be captured. The second one, non-consensual pornography, protects the freedom to dispose of one's intimate image and how it is presented to others. Furthermore, sexual freedom is protected as a secondary object in both instances.[453]

An interesting definitional debate in relation to this offense is what constitutes a naked body: some authors consider it sufficient that some naked body parts are visible with private parts not fully exposed or blurred[454], while others think that at least some private parts (genitals, buttocks, female breasts) must be clearly visible.[455] Body painting does not preclude nakedness and a person without clothes standing sideways or covering their private parts with hands is a naked person for the purposes of the provision.[456] However, people in their underwear, based on available case law, would not be considered naked.[457] Since the provision speaks of a naked person, not just naked body, the doctrine interprets this as a requirement for the person to be identifiable. Both requirements (nudity and identifiability) are satisfied if any part of a naked human body is shown, if at least one person other than the victim can identify her on the image[458], based on any characteristic trait typical to the victim's body.[459] The images do not have to serve a sexual purpose and they can also be recorded with the intention of ridicule, showing ugliness or generally interfering with the private sphere of the person by harmful depictions.[460]

---

[451] Joanna Długosz, 'Art. 216' in Michał Królikowski and Robert Zawłocki, *Kodeks karny. Część szczególna. Tom I. Komentarz do artykułów 117–221* (CH Beck 2013) 825.
[452] ibid 830.
[453] Michał Królikowski and Andrzej Sakowicz, 'Art. 191a' in Michał Królikowski and Robert Zawłocki, *Kodeks karny. Część szczególna. Tom I. Komentarz do artykułów 117–221* (CH Beck 2013) 554.
[454] ibid 556; Marek Mozgawa, 'Utrwalanie Wizerunku Nagiej Osoby Lub Osoby w Trakcie Czynności Seksualnej Albo Rozpowszechnianie Takich Treści' in Jarosław Warylewski, *Przestępstwa przeciwko dorbom indywidualnym* (CH Beck 2012) 487.
[455] Bartłomiej Filek, 'Wizerunek Nagiej Osoby Jako Znamię Przestępstwa z Art. 191a §1 k.k.' [2012] Prokuratura i Prawo 68–75.
[456] Mozgawa, 'Utrwalanie Wizerunku Nagiej Osoby Lub Osoby w Trakcie Czynności Seksualnej Albo Rozpowszechnianie Takich Treści' (n 39) 487.
[457] District Court in Świdnica, Decision from 14 April 2015, II K 497/13.
[458] Filek (n 40) 70.
[459] ibid 67.
[460] Królikowski and Sakowicz (n 38) 556.

Importantly, the criminalization of recording nude or sexual images is limited to a sub-category of non-consensual situations by requiring some form of force, unlawful threat, or deceit. Deceit is understood broadly as any interference with the self-determination of the person in relation to their intimate image.[461] It can for example be installing secret cameras in rooms knowing there will be guests.[462] This is a broader definition of deceit which includes action that not only manipulates the victim to agree to something, but also that prevents the victim from being able to express their will at all. In this wider sense, it is not necessary that the victim knows about being recorded, and therefore all covert forms of recording will qualify as deceitful.[463] Fake castings of models on the other hand would not qualify since they agree to the making of images freely, just not the context of making them, although further publishing of such images would fall under another offence.[464] The literature seems to suggest that private spaces are more protected than public spaces, for instance filming someone nude without their knowledge on a beach, even using zoom on the camera, would not qualify as the offense.[465]

The alternative version of the offence requires publishing, understood widely as making accessible to others, of such images without consent. Here, it is irrelevant whether the perpetrator made the images themselves or got them from third-parties, it is the lack of consent that is relevant. The consent cannot be in the form of a general license to do whatever one wishes to do with the pictures, but has to be given for concrete forms and instances of making the images public.[466]

Visual observation can also intrude upon other privacy-related values, such as secrecy. Poland, in addition to the nudity offence contains a more general provision protecting people from unlawful visual surveillance is the provision of Art. 267(3). The provision does not require any harm to truly occur. Mere attempt to obtain the information by using a technical device is criminalized. These devices would not only include visual recording devices, but also devices which enhance human perceptions, e.g. binoculars. Thus, not only recording, but also technically enhanced observation is criminalized here. The determination whether someone is authorized to some information or not is largely subjective. The confidential nature of the information does not, as a rule, depend so much on the content of the information, but on the preference of people who possess it. This would certainly include the image and sound from private meetings between people[467] and most likely other situations in which people have legitimate expectations of privacy, such as private life in the home. The same provision also protects people from aural and other forms of surveillance. The technical eavesdropping devices covered by the provision contain any devices which allow the perpetrator to obtain the information expressed by sound (speech or recordings), thus covering both recording and overhearing with technical aids.[468] Examples mentioned in the case law include directional microphones, tape recorder, voice recorder and dictaphones.[469] The extent of protected information is also quite broad.

Finally, **Stalking** was not criminalised in Poland until relatively recently, and civil law remedies were used instead. The current Criminal Code has been amended in 2011 to include the criminalization of Stalking in Art. 190a. Stalking is a direct attack on the dignity of the person and also freedom from threats, right to privacy and personal autonomy, and in extreme cases also freedom from inhuman treatment. What is also

[461] ibid 555.
[462] Mozgawa, 'Utrwalanie Wizerunku Nagiej Osoby Lub Osoby w Trakcie Czynności Seksualnej Albo Rozpowszechnianie Takich Treści' (n 39) 488.
[463] ibid.
[464] ibid 490.
[465] ibid 491.
[466] Królikowski and Sakowicz (n 38) 555–556.
[467] Supreme Court Decision, 27 April 2016, III KK 265/15.
[468] District Court in Oława, 9 February 2010, II K 16/10.
[469] Supreme Court Decision, 27 April 2016, III KK 265/15.

at stake is the potential humiliation of the victims, destruction of their reputation and position in the society, especially considering the new possibilities that the modern forms of communications allow and the changing nature of individual's participation in society. It causes similar moral suffering of the victim as physical or mental bullying.[470] Psychological well-being is therefore one of the protected legal goods as well.[471] The protection of individual's dignity requires the protection of an exclusive personal zone where the person is not exposed to "being with others", sharing her experiences and intimate life with them. This protection includes private information related to the individual which guarantees the informational autonomy. It also includes freedom of communications, which includes not only correspondence, but all interpersonal contacts.[472]

The provision is intended to cover unwanted interference with privacy and interference with the feeling of safety of the victim and is also be described as emotional assault.[473] The conduct that is covered is not specified, not even in the form of examples. Doctrine mentions some examples, such as intrusions into private sphere, use of means of communication, unwanted contacts, including those using new information and telecommunication technologies[474], such as excessive texting or emailing[475], as well as persistent commission of petty offences. The conduct can be directed towards the victim or her close relations. The key defining feature is the persistent nature of those actions, it is usually the recurrence of the actions that causes harm to the victim. This harm is manifested in feelings of threat, changes in the usual way of life fear and discomfort which does not allow the victim to live freely.[476]

The criminalized conduct is defined by its consequences: permanent state of stress, fear for one's safety or safety of close persons or the changes in the usual way of life. This is objectivized by requiring these feelings to be 'justified', since the ability of different people to deal with psychological distress varies.[477] It is, however, not fully objectivized, fear is justified if an average person of comparable personal traits as the victim, psychological profile, intellect and mentality would evaluate the situation in a similar way as the victim.[478]

Harassment is defined as behaviour that can objectively result in distress, fear, domination, humiliation or similar negative sensations. It has a combined, multi-action, character, which includes actions of different types and degrees of seriousness. These actions often only qualify when taken together and may be relatively innocent on its own. These actions only qualify as harassment when they are conducted against the will of the victim, which has to be communicated to the perpetrator or objectively evident.[479]

An alternative result requirement to the fear requirement is the violation of privacy can be fulfilled e.g. by recording, photographing, filming, publishing of image, offering companionship or other interference in the physical personal zone.[480] It is not restricted to some places, such as home or dwelling, but refers to the sphere of personal autonomy related to everything in personal life and to avoiding everything that violates personal goods such as health, liberty, honour, name, image or correspondence.[481] The requirement that

[470] Michał Królikowski and Andrzej Sakowicz, 'Art. 190a' in Michał Królikowski and Robert Zawłocki, *Kodeks karny. Część szczególna. Tom I. Komentarz do artykułów 117–221* (CH Beck 2013) 539.
[471] Mozgawa, 'Przestępstwa Stalkingu (Nękania) i Podszywania Się' (n 25) 439.
[472] Królikowski and Sakowicz (n 55) 539–540.
[473] ibid 538.
[474] Ibid.
[475] Court of Appeals Decision, 19 February 2014, II AKa 18/14.
[476] Królikowski and Sakowicz (n 55) 538.
[477] ibid 540.
[478] ibid 543.
[479] ibid 541.
[480] ibid 543.
[481] Explanatory report to the Bill of 25 February 2011 amending the Criminal Code, Nr. 3553.

the harassment violates privacy is not entirely clear. Some authors hold an opinion that each violation of privacy is significant due to the significant of privacy as a legal good itself.[482] A higher threshold is set for public persons,[483] and for instance searching through garbage thrown in the public trash bin by a known person to see how they nourish will not amount to a significant privacy violation.[484]
The principal criminal offence against personal data has been recently inserted in the criminal code in Art. 190a(2)[485], criminalizing **identity theft**, defined as pretending to be another person by using their image or other personal data with the aim to cause material or personal harm to that person. The aim of harming the victim has to be aimed at a specific person. The criminalization of identity theft therefore seems rather restricted, since it would not cover assumed identities that aim to mislead or cause harm to someone else than the person whose identity was taken, and the requirement of specific intent is rather narrow.

Case law

It is difficult to determine what the key cases are, since case law is not a formal source of law in Poland, but in several court cases interesting interpretational clarifications were made.

In relation to the protection of people's intimate visual privacy in Art. 191a, the District Court in Świdnica made clarifications about the meaning of the term 'naked person'. The court clarified that the images do not have to serve a sexual purpose and they can also be recorded with the intention of ridicule, showing ugliness or generally interfering with the private sphere of the person by harmful depictions. However, the Court stated that private parts must be visible, people in their underwear would not be considered naked.[486]

In relation to the provision that protects people from technically mediated surveillance (Art. 267(3)), the Supreme Court made clarifications regarding the meaning of the term 'information not meant for the perpetrator'. The confidential nature of the information does not, according to the Supreme Court, depend so much on the content of the information, but on the preference of people who possess it. This would certainly include the image and sound from private meetings between people.[487] In relation to aural surveillance, the District Court in Oława clarified the meaning of 'technical eavesdropping devices' covered by the provision as any devices which allow the perpetrator to obtain the information expressed by sound (speech or recordings), thus covering both recording and overhearing with technical aids.[488]

In relation to Stalking (Art. 190a(1)), one of the penalised outcomes of persistent harassment is the significant violation of privacy of the victim. This rather vague formulation has been interpreted by the Supreme Court very extensively: "*Privacy itself, regardless of its specific sphere being violated, is a good so significant, that each violation of it is significant.*"[489] The particular case concerned filming and photographing a victim and her children, while on their own property and its vicinity despite their

[482] M Budyn-Kulik, *Kodeks Karny. Komentarz Do Zmian Wprowadzonych Ustawą z Dnia 25 Lutego 2011 r. o Zmianie Ustawy - Kodeks Karny* (LEX 2011) 34.
[483] Królikowski and Sakowicz (n 55) 544.
[484] Marek Mozgawa (ed), *Kodeks Karny. Komentarz* (Wolters Kluwer 2015).
[485] In the same Article as the criminalization of Stalking.
[486] District Court in Świdnica Decision, 14 April 2015, II K 497/13.
[487] Supreme Court Decision, 27 April 2016, III KK 265/15.
[488] District Court in Oława, 9 February 2010, II K 16/10.
[489] Supreme Court Decision, 12 January 2016, IV KK 196/15.

categorical objections, which was considered a significant privacy violation despite the fact the images were not further distributed.[490]

In a case before the District Court in Olsztyn involving prosecution of identity theft (Art. 190a(2)), a woman who copied random photos from the internet to set up a fake account on a gay dating website aiming to make contact with her partner to test his sexual preferences was acquitted, since her aim was not to harm the persons depicted on those photographs, but another person.[491] This shows that the criminalisation of identity theft is interpreted very narrowly by lower courts in Poland.

Significance in practice

When the criminalization of unlawful access to computers was extended in 2008 to cover the pure access cases (without overcoming security measures), Adamski[492] expressed a concern that this would lead to over-criminalisation. A superficial look at the numbers reveals that the number of cases reported to the police rose dramatically from 384 in 2007 to 1513 in 2012.[493] However, I am not in the position that make the assessment, whether the change in substantive law was the main trigger for this increase.

Civil and commercial law

Relevant articles and rationale

The key provisions of the Civil Code protecting personality rights are Art. 23 which establishes this protection and Art. 24 which establishes the remedies for their breach. Art. 23 of the Civil Code reads that personal goods a human being, in particular health, freedom, dignity, freedom of conscience, name or pseudonym, image, privacy of correspondence, inviolability of home, and scientific, artistic, or inventive achievements are protected by civil law. The enlisted personal goods are merely examples, the wording 'in particular' clearly indicates that the list is open to further development resulting from changes in society.[494] Under Art. 24 of the Civil Code, anyone whose personal interests are endangered by another, may demand their actions to cease as long as they are unlawful. In case the personal goods are infringed, the injured party may request that the infringing party takes all actions necessary to remove these effects. The injured party may also demand monetary compensation or that an appropriate amount of money is paid to a public cause. If financial damage is caused, the injured party may demand the payment of financial damages.
Further protection can be found in the Act on authorship rights (*Ustawa o prawie autorskim*). Art. 81 of this Act protects the right of the person to control the public presentation of their image. The dissemination of an image of a person requires the permission of the person depicted. In the absence of an express reservation, no authorization is required, if the person has received payment for posing for the image. No permission is also required to disseminate an image showing a well-known person, if the image was made

[490] Supreme Court Decision, 12 January 2016, IV KK 196/15.
[491] District Court in Olsztyn Decision, 21 July 2015, II K 497/15.
[492] Andrzej Adamski, Opinia do projektu ustawy z druku nr 458 Rządowy projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Opinion on the bill amendment of the Penal Code for the Office of Legal Analyses of the Sejm) http://orka.sejm.gov.pl/rexdomk6.nsf/Opdodr?OpenPage&nr=458.
[493] Adamski , Andrzej, 'Cybercrime Legislation in Poland', National Report for the International Congress on Comparative Law (2015), p. 6. Available at: https://www.researchgate.net/profile/Andrzej_Adamski2/publication/279191115_CYBERCRIME_LEGISLATION_IN_POLAND/links/558d662b08aed6ec4bf34d73.pdf?origin=publication_list
[494] Pryciak (n 15) 223.

in connection to public functions, in particular political, social and professional, or an image in which the person is only one detail of a whole, such as an assembly, a landscape or a public event.

Intermediary liability and duty of care for information society services

The exceptions from intermediary liability are listed in Art. 12-15 of the Act on Electronic Services (*Ustawa o świadczeniu usług drogą elektroniczną*). The provisions are equivalent to those of the E-Commerce Directive.

Indirectly related to this section and interesting as a contrasting approach to the German Network Enforcement Act (See section 3. of the German Country Report):
In Poland, the main concern in relation to social media seems to be not whether they are blocking enough content, but rather that they are blocking too much and too arbitrarily. The private blocking of content in considered a significant problem and the Polish public debate seems to focus strongly on preserving freedom of speech on the internet. This has been translated to actions of public authorities. For instance, the Ministry of Digital Affairs initiated talks with Facebook and in 2018 signed a Memorandum of Understanding, in an effort to strengthen the position of Polish users of Facebook in relation to blocking of their content:

"The Ministry of Digital Affairs, NASK and Facebook, directed by the will to make sure people have access to platforms where they feel safe to share and discuss issues, which are important to them, while being protected from hate speech, violence, bullying and harassment, agree to cooperate in the search of solutions for the multilayered problem of content on the Internet. To that end they have taken joint actions to establish a point of contact designed to submit notifications by Facebook users, whose content, accounts or profiles were removed, with the aim for Facebook to perform an additional review based on its community standards. The Ministry of Digital Affairs as a public entity playing a leading role in the development of the information society and electronic services have initiated this cooperation and will engage in promoting and communicating the contact point".[495]

The proponents of a wider freedom of speech online have also had some success in judicial proceedings against Facebook recently. An organisation called The Social Drug Initiative had content blocked on Facebook, allegedly for breaching the community standards. They took Facebook to court and succeeded with an application for a temporary measure. The court temporarily prohibited Facebook from deleting pages, accounts and groups maintained on Facebook by the Organisation, as well as blocking of individual posts. Facebook is also ordered to keep accounts and pages it previously deleted in case the organisation wins the case, so they can be restored. The court also confirmed that Polish users can assert their rights against Facebook Ireland in Poland and in front of Polish courts.[496]

[495] 'Pierwsze tego typu porozumienie. Ministerstwo Cyfryzacji i Facebook - Ministerstwo Cyfryzacji - Portal Gov.pl' (*Ministerstwo Cyfryzacji*) <https://www.gov.pl/web/cyfryzacja/pierwsze-tego-typu-porozumienie-ministerstwo-cyfryzacji-i-facebook> accessed 23 March 2020.
[496] District Court in Warszawa Decision, 1 June 2019, IV C 608/19.

Regulation of distribution and sales of goods and services

Case law

A number of lower court cases dealt with the protection of people from visual monitoring in relation to protecting appearance as a personal good under the Civil Code (Art. 23). The case law appears to be somewhat inconsistent. For instance, in a case where one neighbour decided to monitor common areas in an apartment complex and saved all the footage on her hard drive, the Court of Appeals in Lublin did not find this to be a breach of personal rights.[497] In a similar case decided by the Court of Appeals in Krakow, the court found violation of personal rights in a case where the neighbour monitored by cameras the outside area in front of his house and part of the area in front of the neighbour's house.[498] The private life considerations in both cases appear to be equivalent, which shows that either there is no uniform standard in which the protection is applied by Polish courts, or the consideration whether personal rights were or not infringed relies on very specific technicalities.

A case which shows the openness of the list of personal goods protected by Art. 23 of the Civil Code and how it is supplemented by judicial decision making is the Supreme Court decision which recognised that the protected personal goods include reputation and good name,[499] values which are not explicitly mentioned in the provision.

Part 3: Mechanisms other than legislation

Non-legal mechanisms

Awareness

The most active in his field in Poland is the foundation Panoptykon. It was founded by a group of lawyers to address the challenges posed by growing surveillance in society. They focus on monitoring and research, advocacy and education. Although their focus seems to be mainly on monitoring of the public authorities, they also monitor the activities of private companies. One of the main goals of the organization is to popularize the knowledge on threats arising with surveillance and suggest various tactics of resistance.[500]

[497] Court of Appeals in Lublin, 20 March 2012, 1Aca 107/12.
[498] Court of Appeals Krakow, 28 May 2014, 1 Aca, 184/14.
[499] Supreme Court Decision, 17 July 2008, II CSK 111/08.
[500] For more on the activities of this organization see: https://en.panoptykon.org/.

16.5 Bijlage 5: Landenrapport Zweden

Auteur: Cecilia Magnusson Sjöberg

Part 1: Introduction

Legal system

The Swedish legal system is based on a civil law tradition. As a consequence of Sweden becoming a member of the European Union by January 1995 the impact of case law has however increased.

The regulatory culture is characterised by a strict norm hierarchical structure. Major categories are fundamental laws – summing up to a constitution – and what may be referred to as ordinary laws decided by the parliament, governmental ordinances, and other provisions issued by public authorities. Adding to the picture is what may be categorised as non-binding general recommendations for practicing law in primarily the public sector of society. This kind of soft law consist of formally non-binding rules. Mention should also be made to an increasing interest in embedded law by way of algorithms mirroring legal rules and regulations that are being coded and run by computers.

The Swedish culture – if such exists in today´s multicultural society – is multifaceted and reflected in legislative measures of different kinds. Of particular interest is the strong heritage of the Swedish principle of openness dating back to year 1766 providing a right of access to public official documents on the one hand and the strong tradition of privacy in terms of data protection on the other. As a matter of fact Sweden was the first country to enact a national Data Protection Act (SFS[501] 1973:289). In this context it is worthwhile mentioning the widespread – and quite often mandatory – use of personal identification numbers (PIN) in both the public and the private sector of society. Common applications comprise identification of individuals for security reasons but also record linkages for the purpose of efficient public administration and commercial profiling of consumers etc.

The court system is quite conventional being based on a general Supreme Court supplemented by an administrative supreme court, including a few special courts. There are also cases decided by lower courts of appeal and district courts. Of importance to privacy by means of data protection is furthermore the Swedish Parliamentary Ombudsmen (JO)[502] supporting individuals and the Swedish Chancellor of Justice (JK)[503] supporting the government.

Fundamental rights framework

Horizontal effect of constitutional law

The Swedish Constitution (cf. above) comprises four fundamental laws and the Riksdag Act (a hybrid regulating the work of the parliament).[504] To begin with, the Instrument of Government contains provisions about the basic principles of the form of government, fundamental rights and freedoms, the riksdag

[501] Svensk författningssamling (Swedish collection of rules and regulations).
[502] https://www.jo.se/en/
[503] https://www.jk.se/other-languages/english/
[504] https://www.riksdagen.se/globalassets/07.-dokument--lagar/the-constitution-of-sweden-160628.pdf

(parliament), the work of the riksdag, the head of state, the government, the work of the government, acts of law and other provisions, financial power, international relations, administration of justice, administration, parliamentary control, local authorities, war and danger of war, and transitional provisions.

Given the question whether current fundamental rights are applicable in horizontal relations the following reference ought to be considered: Chapter 2, provision 6 paragraph 2 Instrument of Government that reads as follows: In addition to what is laid down in paragraph one, everyone shall be protected in their relations with the public institutions against significant invasions of their personal privacy, if these occur without their consent and involve the surveillance or systematic monitoring of the individual's personal circumstances. The wording seems to be pretty clear that horizontal privacy is not included. However the scope of this regulation has over the years been discussed among both scholars and representatives for the ministries. The reasoning boils down to a question whether public institutions are obliged to provide individuals with legal remedies claiming his or her rights to other private parties. The current state of affairs does however indicate that this is not the law-maker´s intention.

Another important fundamental law to comment upon is the previously mentioned Freedom of the Press Act (dating back to year 1766). The Freedom of the Press Act contains provisions about the freedom of the press, the public nature of official documents, the right to anonymity, the production of printed matter, the publication of printed matter, the publication of periodicals, the dissemination of printed matter, offences against the freedom of the press, liability rules, supervision and prosecution, on private claims for damages, court proceedings in freedom of the press cases, matter printed abroad, general provisions, and transitional provisions.

The Freedom of the Press Act is quite complex when it comes to the interaction with the Public Access to Information and Secrecy Act (SFS 2009:400).[505] More precisely, it concerns the Swedish principle of openness and everyone´s right of access to official documents that are public and kept by public authorities. The major rule is that transparency overrules data protection of individuals that might be mentioned in the official documents. There is however an exception, and that is when confidentiality applies and the document(s) in question are (are) to be kept secret by the agency concerned, wholly or partly.

There is no doubt that the principle of openness challenges privacy both in practice and also formally with regard to EU: s legal framework, and in particular the General Data Protection Regulation.[506] In response to this situation the Swedish lawmaker has implemented a provision in Chapter 21 provision 7 of the Secrecy Act (2009:400), which is about confidentiality as a protection of data concerning individuals´ personal conditions regardless of the context.

The rule reads as follow since (2018:2000): Secrecy applies to personal data, if it can be assumed that the data after having been disclosed will be processed in violation of (I) the GDPR or, (ii) the Swedish Supplementary Act (SFS 2018:218) to GDPR, or (iii) the Ethical Vetting Act (SFS 2003:460). So what we have here is a situation where data subjects are at risk for privacy infringements as a result of other data subjects´ constitutional right of access. Actually there is a kind of three party constellation consisting of (a) public agencies keeping personal data (for their case handling) about (b) a variety data subjects that might in their

[505] https://www.regeringen.se/informationsmaterial/2009/09/public-access-to-information-and-secrecy-act/
[506] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

turn be exposed to other private parties´ right of access to their information. From a privacy point of view it is therefore of utmost importance that the secrecy legislation provides a limit to what documents and data are to become public.

Mention should also be made of the Fundamental Law on Freedom of Expression. It includes basic provisions and those on the right of anonymity, on transmission, production and dissemination, on responsible editors, on freedom of expression offences, liability rules, on supervisions, prosecution and special coercive measures, on damages, on court proceedings in freedom of expression cases, on radio programmes and technical recordings emanating from abroad etc., general provisions and transnational provisions.

The Fundamental Law on Freedom of Expression includes in Chapter 1 specific rules about databases granted proof of publication. This authorisation is optional and open for anybody who has applied to the Swedish press and broadcasting authority,[507] paid a moderate fee, appointed an editor, is established in Sweden, keeps track of records and provides a database service that is static (moderated) by the editor and excluding visitors to engage in interactive commenting. Given that an editor who also is controller according to the GDPR (cf. Article 85) engages into personal data processing this activity will according to Swedish legislation be permitted notwithstanding privacy constraints. The horizontal perspective becomes quite clear in situations when registered data subjects are taken advantage of (used) by commercial actors offering database services on the open digital market based on citizens personalized information.

Summing up, the Fundamental Laws of Sweden could lead to privacy infringements in spite of legislation that makes it possible to balance regulatory conflicts of interest. A brief overview shows that the provisions of the Instrument of Government over time, and to a limited extent, has been discussed not only in terms of vertical privacy but also horizontal. The Freedom of the Press Act definitely challenges privacy and data protection due to the principle of openness and the associated right of access to public official documents. However, confidentiality may apply with reference to secrecy legislation. The Fundamental Law on Freedom of Expression makes it legitimate for most parties to acquire a publication permit allowing for personal data processing that otherwise would have been prohibited. The Act of Succession in its turn regulates the order in which descendants of the present King succeed to the throne and has royal but not data protection implications. Neither shows the Riksdag Act any obvious privacy tasks.

Personality rights and fundamental rights protection

In this part of the report it can be noted that the Swedish jurisdiction does not recognize personality rights per se. The Swedish Administrative Act (SFS 2017:900) has however incorporated certain basic values in connection with good administration. The keywords can be seen as common components of the rule of law ("rechtssicherheit"), namely legality, objectivity and proportionality, but this does not fall into to the vertical scope. An illustration of the horizontal perspective could rather be when neighbors use camera surveillance – drones for instance – zooming in ongoing activities.

In spite of the notions of privacy and data protection being common denominators for today´s legal systems Sweden has not chosen a legislative approach to these terms. But this is not similar to saying that the vocabulary is not important. Privacy is commonly understood as being either natural or in principle. With regard to data protection the latter is commonly applied. Yet another perspective has to do with the fact that privacy is not (legally) defined but characterized as a right to be let alone in a private sphere etc.

[507] https://www.mprt.se/en/

Following from the above data protection becomes one aspect of privacy. Furthermore data protection is not only relevant in the legal context of GDPR but also as a kind of information security aspect that needs to be surrounded by different security measures (see for example Article 32 of the GDPR).

Extra legem, intra ius

Algorithmic transparency can serve as an example of a principle that has not yet been codified but nevertheless has emerged in legal doctrine and practice sine the early 1970-ies in the western world. Over the years algorithms have been analyzed and shaped in jurisprudence both as (structured) static problem solving tools (the algorithm does not change during its application) and as dynamic ones. The latter is a typical feature of AI-based solutions based on big data, machine learning, advanced mathematics and statistics, as well increasing computing power with the overall goal of self-improving algorithms.

From the point of view vertical versus horizontal privacy algorithms cannot be pre-defined as supporting one kind especially. It is however a challenge to manage the black box character of self-improving algorithms, that in its term are difficult to match with the rule of law.
Private individuals as well as small enterprises could very well be exposed to algorithms when doing business. Furthermore, algorithms are neither good nor bad in nature but have nevertheless come to play an important role in the digitalization of society and the legal culture being part of it. Nowadays there seems to exist a general understanding emanating from jurisprudence and legal informatics that algorithms are to be illuminated in order to shed light on both vertical and horizontal privacy. The latter could for instance take place in a situation that occurs between a data subject and small businesses.

The reasoning above boils down to a need for algorithmic transparency that can be summarized in the following way. Transparency is a condition for privacy in the context of personal data processing, especially when based on AI-methods. A major keyword here is openness, which however is not equivalent to transparency. This is explained by the fact that an organization may very well be governed by principles of openness but still not provide transparency due to insufficient access rights and lacking implementation of those rights.

Relevant case law (national)

The brief listing below is divided into two parts mirroring the Swedish court system. Generally speaking it consists of one category of general courts deciding cases in commercial and penal cases and another category of courts deciding cases of an administrative character including social insurance, taxation etc.

(a) Supreme Court et al

NJA 2001 p. 409 – Ramsbro Case: Freedom of information and expression versus data protection on the internet in the context of a bank crisis.
NJA 2005 p. 361 – Lundsberg Case: Need for a data subject´ legitimate consent in a work life situation where a boarding school employee and parents are stakeholders.

Court of appeal (Göta hovrätt)

RH 2004:51 – Lindqvist Case: Interpretation and application of core data protection rules on the internet (homepage) regarding sensitive personal data, third country transfers, private processing) etc.
See further EU C-101/01 and Directive 95/46/EC.

(b) Supreme Administrative Court et al

HFD 2011 ref. 77 – Camera surveillance in the entrance of an apartment block not compliant with data protection legislation.
District court (Förvaltningsrätten in Stockholm)
Decision 2 May 2018, Case nr 16590-17 (Right to erasure ("right to be forgotten").

The role of providers and distributors

In order to approach and capture the multifaceted roles of providers and distributors in a digital environment the generic label ICT-suppliers will be used as a base here. The associated descriptive and practically oriented reasoning will shed some light on the nationally oriented comments in this part of the country report. More precisely, emphasis will be made to contractual environments, so called cloud computing and social media.

Sweden has a long tradition of being early adopters of modern ICT. Historically this has taken place in different e-business environments giving rise to data protection concerns but also reducing risks for privacy infringements. Critical factors concerning the horizontal perspective of privacy can in this context to a considerable extent be linked to different business models and contractual clauses agreed upon. Major business models comprise "Business to Business" (B2B), "Business to Consumer" (B2C), and "Business to Government" (B2G). Sweden has furthermore a relatively long tradition of using Standard form contracts. This contractual approach has over the years proven to prioritize the strong parties when it comes to for instance agreed upon personal data processing.

Cloud computing is a common business feature nowadays. There exist no formal (global) definition of this kind of ICT-application(s) that is aimed to dynamically supply digital solutions where and how this can be done as cheap and quick as possible.
Major categories of cloud computing solutions are often made to:

- Public clouds
  - Standardized solution
- Private clouds
  - Customized solution
- Governmental clouds
  - Involving governmental organizations
- Hybrid clouds
  - A combination of several cloud computing solutions

From the point of view of horizontal privacy it is not clear-cut which of the above mentioned business models provide a risk or even threat. In this context it becomes quite clear how important it is to let law play a proactive role. Article 25 in the GDPR regulation about data protection by design and by default is yet another indication of this.

Social media has definitely changed the conditions for horizontal privacy. The list of applications is already rather lengthy and keeps growing. Well-known applications are for instance Facebook, Twitter, Instagram, WhatsApp, and LinkedIn. A common denominator is the transborder character of this kind of ICT supply. From a data subject´s point of view there are therefore a whole set of parties involved. In this context it is primarily important to observe the legal relationship between different private users of the social media. In Sweden the issue of accountability and associated liability is an increasing concern.

Part 2: Protection of privacy and data in horizontal relations

To begin with it is important to clarify that the basis for the analysis is the interplay between privacy and its protection on the one hand and data protection on the other. Privacy could mean many things but in this context it boils down to a right to be let alone in a private sphere. Data protection refers to a means for privacy to the extent that it concerns personal data processing. As a matter of fact personal data protection is also a way to accomplish information security in addition to measures such as confidentiality, integrity, availability, accountability etc. In this report focus is on human privacy (allowing for some reflections concerning small enterprises) by way of data protection in the context of personal data processing. The overall perspective is as already shown directed to so-called horizontal privacy; and here furthermore effectuated through specific legislation.

Data protection legislation

Relevant articles and rationale

In order to respond to the questions raised in this part of the report the overall structure of data protection regulation in Sweden will be briefly presented. At the top of the hierarchical normative structure there is of course the (EU) General Data Protection Regulation (2016/679), the GDPR. Then there is supplementary national legislation: Government Bill 2017/18:105) leading to the Data Protection Act (2018:218) decided by the parliament (Riksdag) that contains rules that are supplementary to the GDPR. Then there is the so-called Supplementary Ordinance decided by the government (2018:219). Adding to the normative picture is furthermore so-called register legislation comprising approximately 200 different legislative acts decided either by the parliament or the government.

This register legislation has to some extent consequences for horizontal privacy. This is explained by the kind of rules and regulations that commonly are laid down in provisions that either support or limit personal data processing in public sector databases. To the extent that personal data are permitted to process by public agencies this could broaden the scope of openness that private parties might claim access to and therefore risk privacy infringements. Critical factors are here the Swedish principles of openness and expression that are not only laid down in fundamental laws but also in Chapter 1 Section 7 of the Supplementary Data Protection Act:

7 § Para 1
EU:s Data Protection Regulation and this Act should not be applied to the extent that it would contradict the Freedom of the Press Act and the Fundamental Law on Freedom of Expression

Another specific rule in national law concerns the infrastructure of horizontal privacy and Article 8 of the GDPR regulating the conditions applicable to child´s consent in relation to information society services, such as social media (Facebook, Twitter, Instagram, LinkedIn etc.).[508] In Chapter 2 Section 4 of the Supplementary Data Protection Act follows that the Swedish lawmaker has decided that a child must be at least 13 years old (EU:s option range 13-16) in order to give his or her consent to personal data processing that takes place in relation to offers of information society services.

[508] According to Article 4(25) of GDPR 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1);

Case law

The heading "Case law" will here be understood broadly referring not only to the major (central) courts within the Swedish legal system, but also another institution offering remedies to data subjects, namely the Parliamentary Ombudsmen (JO, Justitieombudsmannen). Most of JO:s decisions concern vertical privacy and are therefore not relevant here. But there are some interesting borderline decisions that deserve attention. More precisely these concern the distinction between policemen taking an active part in social media, and in particular Facebook. Intention might be to share ideas and experience from the professional work life, however slightly gliding into postings of a private character challenging the privacy of other private individuals:

- JO 2019-01-28 Dnr 119-2018 (Police in social media using ridicule tone)
- JO 2019-03-12 Dnr 7919-2017(Police chief using private e-mail when on duty)

A case that illuminates the interplay between the right of access to official documents, which are public and at the same time includes personal data is commonly referred to as the Mecenate-case (the Patron Case). In spite of dating back some time the principle legal issues are still relevant as laid down in this Supreme Administrative Court decision (reference number RÅ 2002 ref. 54). The case concerned more precisely the company Mecenate´s right of access, directed towards a public agency, to a compilation of personal data about all university students receiving study loan including their home address for the purpose of direct marketing. With reference to Chapter 2 of the Freedom of the Press Act this request fulfilled the legal conditions of an official document, as the compilation was possible to accomplish by so-called routine measures. The fact that the company was going to use the contact data for commercial purposes – direct marketing of a Discount card – did not constitute any legal obstacle as such. The explanation is simply that the scope of the Swedish principle of openness is broad.

The next step was to assess whether the compilation of personal data concerning the students was public or confidential according to applicable secrecy legislation (in particular Chapter 21, provision 7 of the Secrecy Act, 2009:400). Applying current secrecy legislation (including data protection rules) the Supreme Administrative Court found no obstacles referring to confidentiality. With reference to applicable data protection legislation the Court emphasized that the Mecenat Company was not planning to process any sensitive personal data, and that the marketing offer was only to take place once per semester and that there was an opt-out possibility for the data subjects in question. In other words there would be no severe privacy infringement.

Summing up, the case shows that the Swedish principle of openness may be taken advantage of for commercial purposes in spite of being a Fundamental right. The case furthermore shows that secrecy may occur with reference to data protection legislation. This is similar to saying that the lawmaker to a certain extent protects data subjects from other private enterprises. Finally it should be noted that Swedish Law does not (yet) comprise a right of access to public official documents in an electronic format, but only paper based access. The current data protection assessment thus takes place with reference to what can be anticipated to happen after the dissemination of the data compilation.

Actions by the supervisory authority

The Swedish Data Protection Authority (DPA) officially referred to as the Data Protection Authority (Datainspektionen), has played an important role over the years. This relatively small public agency has engaged into regulatory work (to a limited extent though), information and communication activities, and

in particular supervisory measures. Over the years the mission has somewhat changed from achieving a balanced approach to privacy protection on the one hand and freedom of information and expression on the other in to giving priority to the primary goal mentioned. One explanation to this development is possibly the impact of EU:s Data Protection rules and regulations, as well as associated administrative bodies responsible for carrying out a variety of tasks reflecting privacy protection emanating from "Brussels".

One illustration of the increasing impact of the Swedish DPA is about the introduction and use of health apps. It concerns a situation where the Swedish eHealth Agency was assigned by the Swedish government to design and implement a service in the format of a private health account completely based on the data subject´s consent. The infrastructural approach may briefly be described in terms of private individuals being users of health data provided by a whole variety of health data suppliers. The eHealth Agency thus only playing the role of technical intermediate, it was argued. The health data in question would tentatively range from gym data, to medical data. This approach was however not accepted by the DPA, at the time applying the Swedish Personal Data Act, which was the national Act (1998:204) implementing the Data Protection Directive (95/46/EC). Just to mention a few problems the role of controller and/or processor was not clear, the requirement of technical and organizational information security measures were not sufficient. The decision was appealed to the District court of Stockholm, but the DPA:s standpoint remained. So here we have an example of horizontal privacy in the context of a single data subject that according to the lawmaker within the legal system needs protection from other private parties.

See further the decision by the DPA "E-Hälsomyndighetens tjänst Hälsa för mig, 2017-04-21, diarienr 2276-2016" and "Förvaltningsrätten i Stockholm dom 2018-05-24, mål nr 11458-17.

Significance in practice
In the Swedish law making system it can be noted that not only the most central legislation attract serious attention. Regardless of the fact that the general national supplementary data protection legislation does not cover all aspects of the GDPR – rather the opposite – the existing provisions are taken into serious consideration among those that have to apply and comply with the legislation. Adding to the picture is furthermore the large amount of register legislation (see above) that has implications both for vertical and horizontal privacy

An important distinction is rather to be made between provisions in its formal sense (with reference to constitutional law) and other legal guidelines. Practically this has to do with emerging and fast growing soft law. To exemplify, there are vast numbers of recommendations, checklists, FAQs etc. spread in society where the sender could be just anyone promoting data protection measures. There are of course advantages as well as disadvantages associated with this development. For those who are applying data protection law (in a broad sense) in order to be compliant, rules and regulations are commonly much wanted in order to clarify and support the legal state of affairs. From a more general standpoint, taking the rule of law and the principle of legality into consideration, there are instead drawbacks in terms of reduced transparency and democracy when normative actions take place outside of the constitutional scope. Yet another dimension concerns the fact that in a situation of complaints the Data Protection Authority courts of appeal could relatively easy disregard soft law in the context of a conventional trial.

Other

There are two more aspects of data protection legislation worth the attention. The first has to do with how the Data Protection Authority reaches out to the general public by way of actively participating in different kinds of events such as workshops, seminars and conferences. In connection with this kind of occasions it is quite common that public officials representing the DPA takes the standpoint of not only vertical but also horizontal privacy. A rhetoric approach could very well be that nowadays there is reason to watch out not only for the "Big brother" but also "Little sister" or "My Cousin". Yet another observation to be made with regard to the Swedish society is that that public agencies being responsible for (national) archives and associated records management are not at all that visible in the general debate concerning digitalization of society.

Another reflection concerns DSA officials´ participation in public inquires (committees) preceding preparation of government bills, prior to parliamentary decisions about laws to be enacted within the area of data protection. In principle this participation does not formally mirror the DSA practical experience. What it does show though is that the approach among those public officials advocates data protection and not the other way around. Important to observe is that this approach does not only cover vertical privacy but also horizontal. In practice this means that the outcome of legal assessments taking place within the framework of public inquires are to some extent depending of the views put forward on an individual bases. To further illustrate let´s take the example of a review of the legal conditions for personal data processing for research purposes. If the DSA expert does not find research in particular relevant in society he or she most probably will not engage into the create law making process (within the GDPR) enabling for instance research databases. The reasoning above reflects no doubt some challenging aspects of how to balance the objective case official with someone who takes a more personal statement.

Administrative, anti-trust and consumer protection law

The theme of this part of the report will be briefly illustrated by the right to object (to personal data processing according to Article 21.2 of the GDPR reading as follows:

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

To the extent that this statement is directed to vertical and/or horizontal privacy is to some extent an open question. Here the focal point is the latter, which primarily leads to situations involving a data subject in his or her role as a consumer on the one hand and data subjects in the format of a small commercial enterprise that under certain conditions would also fall within the scope of the GDPR. So in this scenario we would have one private individual buying or selling, which involves personal data processing, and another one doing the same but the other way around. This implies actions between two different private individuals, and a relationship with one clearly qualifying as a data subject according to the GDPR and another one that sometimes but not always is to be categorized as a data subject and not a (commercial) data controller or processor.

In a broad perspective much of the governing consumer legislation regarding B2C is found in the national E-commerce act (2002:562). Considering that this law explicitly is exempt from personal data processing it

will not be further analysed here.[509] In terms of national legislation a set of provisions in the Swedish Marketing Act (2008:486) will instead serve as an example.[510] The business model here is that of a consumer data subject, and a (small) trader whose personal data processing falls within the scope of data protection legislation. The rules concern unsolicited advertising.

Section 19
A trader may, in the course of marketing to a natural person, use electronic mail, a telefax or automatic calling device or any other similar automatic system for individual communication that is not operated by an individual, only if the natural person has consented to this in advance. Where a trader has obtained details of a natural person's electronic address for electronic mail in the context of a sale of a product to that person, the consent requirement stipulated in the first paragraph shall not apply, provided that,
1. the natural person has not objected to the use of the electronic address for the purpose of marketing via electronic mail,
2. the marketing relates to the trader's own similar products and
3. the natural person is clearly and explicitly given the opportunity to object, simply and without charge, to the use of such details for marketing purposes, when they are collected and in conjunction with each subsequent marketing communication

Section 20
In marketing via electronic mail the communication shall at all times contain a valid address to which the recipient can send a request that the marketing cease. This also applies to marketing to a legal person.

Section 21
A trader may use methods for individual distance communication other than those referred to in Section 19, unless the natural person has clearly objected to the use of such methods.

In this context mention could be made of the scope of children´ consent according to Chapter 2 Section 4 of the Swedish Data Protection Act that reads (roughly translated);

When offering information society service directly to a child living in Sweden processing of personal data is permitted based on the child´s consent, provided that the child is at least 13 years. If the child is less than 13 years, such processing shall only be permitted if consent is given or accepted by the person who has parenthood for the child.

Criminal law

The structure of criminal law in Sweden can briefly be outlined as follows from the listing below, mirroring applicable core legislation. Do note that it is not complete and merely intends to illuminate the regulatory approach from the point of view of digitalisation. The horizontal perspective of privacy becomes visible when criminal actions involve primarily and/or exclusively private individuals.

General penal legislation

- The Swedish Criminal Law (1962:700)
    - *Technically neutral provisions*

Examples:

[509] See Section 1 paragraph 2 "Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster".
[510] https://www.government.se/government-policy/consumer-affairs/the-marketing-act-marknadsforingslagen/

- On offences against liberty and peace, Chapter 4 – Section 6 a ("kränkande fotografering")

A person who unlawfully, by means of a technical device, covertly records an image of a person who is indoors in a home, or in a toilet, dressing room or other similar space, is guilty of **intrusive photography** and is sentenced to a fine or imprisonment for at most two years.

- On defamation, Chapter 5, Section 1 ("förtal")

A person who identifies someone as being a criminal or as having a reprehensible way of life, or otherwise provides information liable to expose that person to the contempt of others is guilty of ***defamation*** and is sentenced to a fine.

- *ICT adjusted provisions*

Examples:[511]

- On offences against liberty and peace, Chapter 4 – Section 6 c ("olaga integritetsintrång")

A person who intrudes into the private life of another person by disseminating:
1. an image of or other information about a person's sexual life;
2. an image of or other information about a person's state of health;
3. an image of or other information about a person being subjected to an offence that includes an attack on their person, liberty or peace;
4. an image of a person in a very vulnerable situation; or
5. an image of a person's wholly or partially naked body,is, if the dissemination is liable to result in serious damage to the person whom the image or information concerns, guilty of unlawful **breach of privacy** and is sentenced to a fine or imprisonment for at most two years.

- *On offences against liberty and peace, Chapter 4, Section 9 c § ("dataintrång")*

A person who unlawfully obtains access to information intended for automatic processing, or unlawfully alters, erases, blocks or, in a register, inserts such information, is guilty of ***breach of data security*** and is sentenced to a fine or imprisonment for at most two years. The same applies to a person who seriously disturbs or impedes the use of such information in an unlawful way through some other, similar measure

- Criminal Data Act (2018:1177)[512]

Specific penal legislation

Examples:

- Act (1998:112) on Responsibility for Electronic Bulletin Boards[513]
- Camera Surveillance Act (2013:460), Sections 45-46, Penalties etc.

[511] About Net violations see e.g. Axberger, H-G. Nätkränkningar som rättsligt och demokratiskt problem. Institutet för juridik och internet, Skrifterserie nr 1, 2018.

[512] Implementation of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[513] Translated into English by Jacob Palme
https://people.dsv.su.se/~jpalme/society/swedish-bbs-act.html

The above-mentioned BBS-Act[514] is interesting for several reasons. It was in force already in year 1998, at the time when the Internet and World Wide Web were barely existing.
The Swedish lawmaker was quite thoughtful whether to keep the BBS-Act or not, but decided to do so. As it turns out the BBS legislation has made kind of comeback in case law during the last couple of years in combination with Swedish general penal legislation. The structure of the BBS-is chapter wise as follows:

- Areas of application
- Information to users
- Supervision of the service
- Obligation to remove certain messages
- Penalties, and
- Forfeiture

Especially noteworthy in order to understand the scope of this legislation is to begin with its orientation towards interactive services, i.e. not those that are moderated in beforehand. The information duty on behalf of the supplier comprises each person who wishes to use the service about his or her identity and to what extent their messages will made available to other users. Of particular relevance for the running of the service is the requirement to keep the service under supervision, not necessarily on a 24/7 bases but as much as is needed. Should there occur illegal messages those have to be removed. Furthermore, the BBS-Act includes provisions about penalties and forfeiture.

In the previous data protection legislation the so-called Personal Data Act (1998:204) was the Swedish core law implementing the EU Data Protection Directive (95/46/EC). The Act contained a provision about penalties in Section 49:

A person who intentionally or by carelessness
a) provides untrue information in such information to registered persons as is prescribed by this Act, or in the notification to the supervisory authority under Section 36 or to the supervisory authority when the authority requests information in accordance with Section 43,
b) processes personal data in contravention of Sections 13–21,
c) transfers personal data to a third country in contravention of Sections 33–35, or
d) omits to give notification under Section 36, first paragraph, or in accordance with regulations issued under Section 41, shall be sentenced to a fine or imprisonment of at most six months or, if the offence is grave, to imprisonment of at most two years.

A sentence shall not be imposed in petty cases.

A person who has contravened an order subject to a default fine in accordance with Section 44 or 45, first paragraph, shall not be sentenced for liability for an act that is subject to the default fine order.

As a result of the EU Data Protection Reform the Swedish lawmaker changed standpoint.[515]
The current supplementary national legislation does not contain any provisions about penalties. This could however been an option with reference to the regulatory scope of the Member states (Article 84 in the GDPR). In Sweden however the regulation in GDPR about right to compensation and liability (Article 82),

[514] Bulletin Board Systems
[515] See further Government Bill 2017/18:105, Ny dataskyddslag (New Data Protection Act) pp 143 ff.

and (Article 83) about general conditions for imposing administrative fines (Article 83) were found satisfactory.

References to two relatively recent cases decided by the Supreme Court illuminating criminal law in digital environment:

- Supreme Court Verdict NJA 2018 s. 562, the so-called Facebbok case
  "Ett yrkande om ansvar för underlåtenhet att avslöja brott ska ogillas om yrkandet är alternativt till ett yrkande om ansvar för delaktighet i brottet. – En sändning på internet som i allt väsentligt är obestämd till format, inriktning och tid är inte förenad med skydd enligt 1 kap. 6 § yttrandefrihetsgrundlagen (webbsändningsregeln)."
  (Google translate: "A claim for responsibility for failure to disclose a crime must be rejected if the claim is an alternative to a claim for responsibility for participation in the crime. - An internet broadcast that is essentially indeterminate in format, orientation and time is not associated with protection in accordance with Chapter 1. § 6 Statement of freedom of expression (webcasting rule)."
- Supreme Court verdict Stockholm 15 March 2020 in case number 5438-19; about breach of privacy ("olaga integritetsintrång") on Instagram in connection with sickness in a bar environment.

Civil and commercial law

It is difficult to point at specific rules concerning privacy and data protection that are meant to be applied entirely in horizontal relations. Some examples are however included in other parts of the report. One aspect to bring forward has to do with the fact that it is nowadays not that obvious what is to be understood as – pure – civil and commercial law in comparison with for instance public and administrative law. What does emerges as relevant, not least from a Swedish point of view, is rather an approach oriented towards infrastructures and the impact information and communications technologies have on the development. Generally speaking infrastructures can be either hard, e.g. road and traffic nets including broadband, or soft, e.g. social networks. A more holistic view implies that there are also legal infrastructures undergoing changes in response to the surrounding society. More precisely this is shown in relation to in particular data processing becoming automated, communication taking place in (transborder) digital networks and documentation by way of electronic measures.

Within this framework horizontal privacy in the context of data protection is a perspective of its own kind to be contrasted to vertical privacy. The Swedish experience is for instance shown by way of a regulatory structure – flexible to EU law – that embodies basic conditions for communications. The current core national legal sources are:

- The Electronic Communications Act (20003:389)
  - Government bill (2002/03:110)
- Better rules for Electronic Communications:
  - Government bill 2010/11:115

To further illuminate see below the structure of the Act:

Chapter 1	General provisions
Chapter 2	Notification
Chapter 3	Right to use radio frequencies and numbers

Chapter 4	Interconnection, etc.
Chapter 5	Services to end-users etc.
Chapter 6	Protection of privacy
Chapter 7	Supervision, etc.
Chapter 8	Consideration of matters
Transitional provisions	

There is one provision that deserves particular attention and that is Chapter 6 Section 18 that explicitly address requirements of privacy. For instance, the use of cookies does not only require information to be given to data subject but also his or hers consent. No doubt this regulation gives rise to questions concerning the borderline between electronic communications and the more general regulation as laid down in the GDPR (including national supplementary legislation). Attention should also be paid to on-going regulatory work implementing Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, which has resulteer in a Swedish memorandum (752 pages) concerning the introduction of a codex for electronic communication. Intention is that the new national framework based on this Act shall be in force by December 21, year 2020.[516]

Part 3: Mechanisms other than legislation

Non-legal mechanisms

Awareness

Outside of legislative initiatives awareness of privacy related to data protection, is in particular endorsed by The Swedish Institute of Law and Internet (IJI).[517] On the homepage the institute describes itself as "a Swedish expert organisation working with privacy online, with special focus on protecting individuals from online abuse, threats and harassment". More precisely this is to be accomplished by three different approaches, namely

(a) providing free legal counsel to victims of online abuse
(b) raising awareness on what the right to privacy covers in online settings, and
(c) lobbying work.

The activities of IJI should not be mixed-up with IRI, i.e. The Swedish Law & Informatics Research Institute (IRI) at the Faculty of Law, Stockholm University.[518] In contrast to IJI and its network oriented organization, the Swedish Law & Informatics Institute plays a formal part of the University appointed and monitored by the Faculty and the President. In this context the work of IRI is valuable as privacy is a major theme for a variety research activities e.g. doctoral and post docs, national and international projects, workshops, conferences, expertise participation in governmental inquiries, and commercial settings. Awareness can also be linked to the Swedish Association for IT & Law (SIJU).[519] This association emanates from the early days of a Working Party for Computers of Law hosted by Stockholm University

[516] https://www.regeringen.se/4adaf8/contentassets/ea974788bbac4e3bbe80ba866524c3f2/pm-genomforande-av-direktivet-om-inrattande-av-en-kodex-for-elektronisk-kommunikation.pdf
[517] http://www.juridikinstitutet.se/home-english/, Institutet för juridik och internet
[518] https://irilaw.org, Institutet för rättsinformatik
[519] https://siju.se/ Svenska föreningen för it & juridik

(established in year 1968). Now it is a society primarily meeting legal practitioners quest for updates on legal developments not least within the area of privacy and data protection.
It all boils down to an understanding of the importance of awareness based on professional knowledge that in its term can be conveyed to the general public being major stakeholder.

Self-regulation
The meaning of self-regulation is not obvious but is rather contextual. Here the understanding is broad, including soft law in terms of non-binding rules issued by a variety of stakeholders. Commonly self-regulation is a way of creating more but also purposeful guidance about how to interpret and apply law in practice. Often but not always, self-regulation is a fruitful method in response to the traditional lawmaker not being able to respond rapidly enough to current needs in society. It can be argued that the area of privacy and data protection is such an environment.

One initiative worth illuminating is referred to as eSam[520] promoting eCollaboration.[521] The overall ambition of this organization is to actively involve primarily representatives for the public sector in cross border activities in particular within the areas of data protection, secrecy and information security. eSam is based on memberships currently comprising 27 public agencies and the Swedish Association of Local Authorities and Regions (SKR).[522] Roughly translated from eSam´s homepage its members want to take advantage of the potentials of digitalization in order to facilitate activities of private individuals and companies by way of efficient use of common resources. One important outcome of eSam concerning privacy is their so called legal statements about for instance applied confidentiality and data protection rules within commercial business models such as cloud computing.

Data protection forum is yet another organization that deserves attention within the framework of self-regulation.[523] Formally speaking it is a non-profit association aiming to clarify and strengthen the role of data protection officers (DPO). The forum has achieved broad recognition in connection to the yearly international conference referred to as the Nordic Privacy Arena.

Another kind of self-regulation is found in the private sector emerging from business law firms. One example hereof is Delphi engaging into data protection by way of a tech blog.[524] In this context there is room for both horizontal and vertical privacy.

Other mechanisms

Education may be conceived of as a non-legal mechanism with a high impact factor when it comes to privacy. To exemplify, the Stockholm University Law Program includes mandatory training in data protection law. This takes place throughout a four months course during the seventh semester, i.e. at advanced level. Furthermore, there are elective courses addressing IT law and Cyber Law even more specifically, also offering composition of exam theses.

[520] The acronym eSam is short for electronic collaboration.
[521] http://www.esamverka.se/om-esam.html
[522] https://skr.se/tjanster/englishpages.411.html
SKR is a non governmental organisation (NGO)
[523] https://dpforum.se/
[524] https://www.delphi.se/sv/tech-blog-kategorier/dataskydd-och-personuppgifter/

Quite a lot of pedagogical efforts are placed on how to distinguish between the right to privacy and data protection in horizontal relations as opposed to vertical privacy. The latter is illuminated during lectures (digital as well as conventional oral ones), seminars, exercises and e-exams. Students are trained to apply a comprehensive methodological approach in order to understand the different roles of a controller, processor, data subject etc. To exemplify, a theme addressed could be a scenario where a small business plan to launch an app for the purpose of e-health. In spite of such a product being based on consent on behalf of the consumer quite a few data protection issues will arise. What about fundamental data protection principles such purpose limitation, security measures, information duties etc.?

16.6 Bijlage 6: Landenrapport Vereningd Koninkrijk

Auteur: Lorna Woods

Part 1: Introduction

Legal system

The United Kingdom is a monarchy. The Head of State is the Queen and one chamber of the legislature (the Lords) is not elected. The United Kingdom does not have a written constitution; the courts have recognised that some statutes have a constitutional status, notably the Human Rights Act 1998[525], which incorporates the European Convention on Human Rights, though even these can be repealed by the express intention of Parliament.
Note some matters are dealt with by Royal Charter[526], so the Press Recognition Panel set up following the Leveson Inquiry was granted a Royal Charter (see 8.2). There is no separate constitutional court; the highest court is the Supreme Court. The legal tradition is common law – though a considerable amount of law is now found in statute and statutory instruments.

The regulatory culture is mixed in terms of regulation and examples of all types of regulation can be found in the media field (e.g. broadcasting with Ofcom empowered to regulate by the Communications Act 2003[527]), co-regulation (advertising with the ASA being 'backed up' by Ofcom[528] in re broadcast advertising and trading standards[529] more generally) and self regulation (press - IPSO). There has been a movement since the coalition government towards 'removing red tape' (see Better Regulation Executive).

In general terms, the courts have repeatedly held that all human rights are equal (especially as regards freedom of expression and privacy)[530], it is noticeable that there are special provisions as regards freedom of expression in the Human Rights Act. As the Supreme Court made clear in *PJS*, s 12 Human Rights Act does not enhance the weight which Article 10 rights carry. The United Kingdom certainly does not not

[525]Available: https://www.legislation.gov.uk/ukpga/1998/42/contents
[526]The Privy Council provides a brief introduction, here: https://privycouncil.independent.gov.uk/royal-charters/
[527]Available: https://www.legislation.gov.uk/ukpga/2003/21/contents
[528]The relationship is detailed in a memorandum of understanding, available: https://www.asa.org.uk/uploads/assets/23cc61df-e57c-4957-81ac15378b7730b7/mou-asa-ofcom.pdf
[529]Details of the ASA's use of trading standards powers can be found here: https://www.asa.org.uk/codes-and-rulings/trading-standards-referrals.html
[530]*Re S (A Child)(Identification: Restrictions on Publication)* [2005] 1 AC 593 (available: https://publications.parliament.uk/pa/ld200304/ldjudgmt/jd041028/inres-1.htm), para 17; see also *Re W* [2006] 1 FLR 1, para 53.

focus on human dignity, though the courts occasionally mention related ideas (flagged up in text); by contrast, open justice is a fundamental constitutional principle.[531]

There are a number of regulators in the United Kingdom, in particular in relation to privatised utilities. It is notable that Ofcom has a very broad remit, covering broadcasting and VOD (and implementation of VSP provisions under revised AVMS Directive); spectrum; telecommunications and post. It will be given responsibilities in relation to online harms. The Information Commissioner and her office (ICO) deal with data protection and freedom of information. The ICO has increased in size significantly since the GDPR. Note also the existence of the Equality and Human Rights Commission which supports the implementation of the Equality Act 2010 (which applies horizontally as well as to public bodies).

Fundamental rights framework

Horizontal effect of constitutional law

The horizontal effect of the Human Rights Act (HRA) was initially the subject of some debate.[532] Section 3 HRA states that courts should interpret legislation in the light of the ECHR. Under s. 6 HRA courts, as public authorities, are required to comply with the requirements of the ECHR. A judgment should be Convention compatible even when it relates to litigation between two parties. The starting point for the case law on this was a privacy action: *Douglas v Hello*[533], followed by *Campbell v MGN*[534] (see further 2.4).

Personality rights and fundamental rights protection

There is no specific personality right - though the case law on privacy and personal information has developed rapidly with the introduction of the Human Rights Act (see below). That case law has recognised that Article 8 may have two distinct components: "unwanted access to private information and unwanted access to one's ... personal space".[535] The second category is sometimes considered to be about intrusion or acquiring information.

Note also the protection granted through the Equality Act: while not aimed at protecting personality rights, it aims to protect people by reference to points of difference which may play into identity (e.g. sex, race, religion, disability).

[531] *Scott v Scott* [1913] AC 417, 463-464; *AG v Leveller Magazine* [1979] AC 440, 450; *Cape Intermediate Holdings Ltd* v *Dring (for and on behalf of Asbestos Victims Support Groups Forum UK)* [2019] UKSC 38, esp paras 41-44, available: https://www.supremecourt.uk/cases/uksc-2018-0184.html

[532] See e.g. Murray Hunt 'The Horizontal Effect of the Human Rights Act' [1998] *Public Law* 423; Sir William Wade, 'Horizons of Horizontality' [200] *Law Quarterly Review* 217; Dawn Oliver, 'The Human Rights Act and the public law/private law divide' [2000] *European Human Rights Law Review* 343. For a more extensive and recent treatment see e.g. Jane Wright *Tort Law and Human Rights* (2nd ed) (Hart Publishing: Oxford, 2017).

[533] [2005] EWCA Civ 595; [2005] 3 WLR 881

[534] *Campbell v MGN* [2004] UKHL 22; [2004] 2 AC 457, available; http://www.bailii.org/uk/cases/UKHL/2004/22.html

[535] *PJS*, para 58, available: https://www.supremecourt.uk/cases/docs/uksc-2016-0080-judgment.pdf

The Protection from Harassment Act 1997[536] (PHA) contains a civil cause of action in relation to harassment as well as the criminal offences in relation to England.[537] Harassment is not defined in the PHA although s. 7(2) explains that the term includes "*alarming the person or causing the person distress*". It seems that harassment has the same meaning in the context of the criminal offence as the civil action. In *Thomas v News Group Newspapers* Lord Phillips defined harassment as "*conduct targeted at an individual which is calculated to produce the consequences described in section 7 and which is oppressive and unreasonable*".[538] In *Iqbal*, however, Rix LJ said:

A professional man's integrity is the lifeblood of his vocation. If it is deliberately and wrongly attacked, whether out of personal self-interest or malice, a potential claim lies under the Act"[539]

This ruling has raised some questions about the relationship of harassment with defamation. The claimant does not have to be directly targetted but be a person to whom alarm or distress were objectively foreseeable.[540] Closely connected groups may also be subjected to 'collective' harassment (and this is not limited to 'protected characteristics' as defined in relation to discrimination). Harassment requires a course of conduct meaning conduct on at least two occasions, and it is the course of conduct which is to constitute harassment not the individual instances.[541] The individual circumstances themselves do not need to be contrary to the law. It has been argued that leaving content up online (after receipt of notification of problematic nature of content) could constitute harassment.[542]

There is a statute dealing with data protection: the Data Protection Act 2018 (DPA18), replacing the Data Protection Act 1998. It 'implements' the GDPR and the Law Enforcement Directive; it also deals with data protection and the security services. The data protection rights of action are distinct from causes of action linked to Article 8 ECHR and based in case law (discussed 2.4).

Defamation has to a large extent been codified. The most recent legislation in England is the Defamation Act 2013[543]; parts of the Defamation Act 1952 and Defamation Act 1996 remain in force. Defamation protects the reputation of the claimant.[544] The 2013 Act brought in a number of important changes aimed at ensuring a 'fair balance' is struck between freedom of expression and the protection of reputation against a background in which concerns had been expressed about 'libel tourism'. Note, the Defamation Act 2013 does not affect law in Scotland or Northern Ireland. A key change is that a statement (whether libel or

[536A]vailable: http://www.legislation.gov.uk/ukpga/1997/40/contents
[537]In Scotland it is possible to bring a claim for damages in relation to s 8 PHA
[538]*Thomas v News Group Newspapers* [2001] EWCA Civ 1233, available: https://www.bailii.org/ew/cases/EWCA/Civ/2001/1233.html; see also *Majrowski v Guy's and St Thomas' NHS Trust* [2006] UKHL 34, [2007] 1 AC 224, available https://www.bailii.org/uk/cases/UKHL/2006/34.html. A slightly different formulation can be found in *Hayes v Willoughby* [2013] UKSC 17, available: https://www.bailii.org/uk/cases/UKSC/2013/17.html
[539] *Iqbal v Dean Manson* [2011] EWCA Civ 123, para 42 available: https://www.bailii.org/ew/cases/EWCA/Civ/2011/123.html
[540]*Levi v Bates*
[541] *Iqbal v Dean Manson*
[542]*Galloway v William Frederick Frazer, Google Inc t/a YouTube and others* [2016] NIQB 7, available: https://judiciaryni.uk/judicial-decisions/2016-niqb-7
[543]The explanatory notes are available here: https://www.legislation.gov.uk/ukpga/2013/26/notes
[544]For discussion of the impact of privacy see e.g. Mullis and Scott "The Swing of the Pendulum: Reputation, Expression and the Recentering of English Libel Law" (2012) 63 *NILQ* 27; Howarth "Libel: its purpose and reform" (2011) 74 *Modern Law Review* 845

slander) is no longer defamatory unless a claimant can show that '...its publication has caused or is likely to cause serious harm to [his/her] reputation…'. The issue of serious harm was considered by the Supreme Court in *Lachaux*.[545] The test was to be understand against the background of the common law approach -essentially that *"the words tend to lower the plaintiff in the estimation of right-thinking members of society generally"*.[546] In *Lachaux*, the Supreme Court held that following the 2013 Act the words complained of must not only be inherently injurious but *must also be shown to produce serious harm in fact*. The English courts had previously held that trivial claims should not be brought and that in some contexts (e.g.chat rooms) publication does not have the gravity of a written libel.[547] Bodies trading for profit must additionally show that a statement has caused, or is likely to cause, serious financial loss. There are four defences: truth (formerly 'justification'); honest opinion (replacing the common law test of fair comment); public interest (codifying the jurisprudence starting with *Reynolds*[548]); and privilege. There are special defences for, *inter alia*, website operators (see below).

In *Charleston*, the images of the heads of two actors in a television soap were superimposed on images of a man and woman who appeared to be having sex as part of a pornographic computer game, and a photograph from which was published by a newspaper. The claimants were unsuccessful as the newspaper article made it clear the image was altered and was critical of the game-makers.[549]

Extra legem, intra ius

There are a number of doctrines developed by the courts which can be used to protect personality rights/privacy, but there is a question as to the extent to which fundamental rights themselves are protected by the common law (including equity). Before the introduction of the HRA, the courts interpreted national law – both statutory and case-based in line with international law obligations where possible; this includes human rights obligations. In some cases the appellate judges have emphasised that the common law comprises respect for fundamental rights.[550] Whether this is actually the case and specifically whether all rights would be treated equally is another question.

[545] *Lauchaux v Independent Print* [2019] UKSC 27, available: https://www.bailii.org/uk/cases/UKSC/2019/27.html
[546] *Lachaux* para [6], citing *Lord Atkin in Sim v Stretch [1936] 2 All ER 1237, 1240*
[547] *Tamiz v Google* [2013] EWCA Civ 68, [2012] EWHC 449 (QB) but note libel can occur via Twitter: *Monroe v Hopkins* [2017] EWHC 433 (QB) and in re Facebook: *Stocker v Stocker* [2019] UKSC 17, available: https://www.supremecourt.uk/cases/docs/uksc-2018-0045-judgment.pdf.
[548] *Reynolds v Times Newspapers* [1999] UKHL 45, available: https://www.bailii.org/uk/cases/UKHL/1999/45.html; *Flood v Times Newspapers* [2012] UKSC 11, available: https://www.bailii.org/cgi-bin/format.cgi?doc=/uk/cases/UKSC/2012/11.html
[549] *Charleston & Smith v News Group Newspapers Ltd* [1995] 2 AC 65; [1995] 2 WLR 450; [1995] 2 All ER 313
[550] See e.g. views of the Supreme Court in *R (Osborn) v Parole Board* [2013] UKSC 61; *Kennedy v The Charity Commission* [2014] UKSC 20; *R (HS2 Action Alliance Ltd)* v *Secretary of State for Transport* [2014] UKSC 3, [2014] 1 WLR324; *A* v *BBC* [2014] UKSC 25, [2014] 2 WLR 1243; *R (Evans)* v *Attorney General* [2015] UKSC 21. See further Brice Dickson, *Human Rights and the UK Supreme Court* (Oxford University Press: Oxford, 2013); Roger Masterman and Se-shauna Wheatle, 'A Common Law Resurgence in Rights Protection?' [2015] *European Human Rights Law Review* 57; Richard Clayton, 'The Empire Strikes Back' [2015] *Public Law* 3.

The courts have recognised that the common law protects freedom of expression,[551] although the decisions of the courts have not always matched the approach under the ECHR.[552] In *Wainwright v Home Office*,[553] the House of Lords recognised privacy as an underlying value only; in the earlier *Smith* case[554] concerning a different aspect of Article 8, the domestic courts also failed to recognise the right. These, however, are pre-HRA decisions. It may be argued that the common law itself has been changed by the HRA in a way that is not dependent on the continued existence of the HRA (see 2.4). More generally, there have been concerns about relying on the common law, partly because the list of rights protected are not clearly delineated. Nonetheless, it seems that the current practice is to plead HRA arguments and the common law in the alternative, as can be seen in *PJS*.[555]

Relevant case law (national)

There are a number of causes of action that could be used to protect against invasions of privacy, both in statute and derived from the common law; some overlap (this is not unusual).[556] There is no requirement that the claimant should pursue the most 'appropriate' or obvious claim; nor can the defendant complain about and disadvantage suffered through that choice.[557] Applicants can (and do) bring an action relying on multiple causes of action.

The requirements to show breach of ***confidence***[558] were set down in *Coco v A N Clark (Engineers) Ltd.*[559] *They* require that:

- the information has the necessary quality of confidence (ie it is not public knowledge[560]);
- it was imparted in a manner which imposed an obligation of confidence (this often arises from a relationship, but can also arise from contract and the circumstances of the disclosure[561]); and
- there has been unauthorised use to the detriment of the person whose information it was[562].

By contrast to e.g. Data Protection Act[563], confidentiality can apply to oral disclosures as well as written. Disclosure of confidential information may take place if the individual to whom the information relates has consented; where disclosure is in the public interest (and freedom of expression may play a role here); or

[551] See e.g. *R v Secretary of State for the Home Department, ex parte Brind* [1991] 1 AC 696 (HL); *R v. Secretary of State for the Home Department, ex parte Simms* [2000] 2 AC 115(HL)
[552] Contrast approach of the Supreme Court in *Kennedy*, supra, with that of the European Court of Human Rights in *Magyar Helsinki Bizottság v Hungary*, 8 November 2016.
[553] [2004] 2 AC 406.
[554] *R v Ministry of Defence, ex parte Smith* [1996] QB 517 (CA).
[555] *PJS* v *News Group Newspapers Ltd* [2016] UKSC 26.
[556] On relationship between misuse of private information and defamation see *Hannon v News Group Newspapers* [2014] EWHC 1580 (Ch) paras [25]-[28]; *ERY* v *Associated Newspapers Ltd* [2016] EWHC 2760 (QB), paras [66]-[68].
[557] *Joyce v Sengupta* [1993] 1 WLR 337 CA, per Nicholls VC (p. 348).
[558] The precise categorisation of breach of confidence has been the subject of some debate – see e.g. Law Commission, Breach of Confidence (Law Com. No 110) (Cmnd 8388), October 1981, available: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2016/08/LC.-110-BREACH-OF-CONFIDENCE-REPORT-ON-A-REFERENCE-UNDER-SECTION-3le-OF-THE-LAW-COMMISSIONS-ACT-1965.pdf. The starting point is often given as *Prince Albert v Strange* (1849) 1 Mac. & G 25.
[559] *Coco v A.N. Clark (Engineers) Ltd* [1969] RPC 41, 47.
[560] *Mosley v. News Group*; cf *PJS & YMA v MGN* [2016] UKSC 26 (a claim of misuse of private information)
[561] See *Douglas v Hello!*
[562] This point is generally accepted, though there is some discussion as to whether proof of detriment is required – see *Cf Partners* (below), para 142
[563] In re Data Protection Act 1998: *Scott v LGBT Foundation Ltd* [2020] EWHC 483 (QB), available: https://www.bailii.org/ew/cases/EWHC/QB/2020/483.html

where there is a legal duty to do so (e.g. court order). Note also confidence can also protect business secrets not just information relating to individuals.[564] Confidence has been used in cases were a photographer used images he was commissioned to take without the subjects' permission,[565] though the jurisprudence did not provide much protection for those in a public place. This is why the *Campbell* case was so ground-breaking.

The doctrine of ***misuse of private information***, which is concerned with the communication of private information, was first introduced in *Campbell v MGN*. The Court established a two-stage test:

- privacy of the information (the reasonable expectation of privacy); or,
- if there is room for doubt whether information is private, if disclosure of the information about the individual concerned would give substantial offence to a person of ordinary sensibilities placed in similar circumstances to that individual.

Significantly, the House of Lords argued that:

> Instead of the cause of action being based upon the duty of good faith applicable to confidential personal information and trade secrets alike, it focuses upon the protection of human autonomy and dignity - the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people.[566]

The defence most frequently relied on is that the claimant's right to privacy is outweighed by the defendant's right to freedom of expression under Article 10 of the Convention or is in the public interest, including the public interest in setting the record straight[567] or the right of an individual to tell his story.

In *Murray*[568], which like *Campbell* concerned photography in a public place, the Court identified a number of factors:

- attributes of the claimant;
- the activity in which the claimant was engaged;
- the location;
- the nature and purpose of the intrusion;
- consent;
- effect on the claimant;
- circumstances in which the publisher obtained the information.

In principle, photographs of people in the street could give rise to an expectation of privacy, depending on the circumstances. *Murray* concerned the child of a celebrity; in *Weller*, the Court said that although in principle the rights of adults and children are the same, there are several considerations which are relevant to children which may mean that in a particular case a child has a reasonable expectation of privacy where an adult does not.[569] Photographs are considered particular sensitive (by comparison to text).[570]

---

[564] See e.g. *CF Partners (UK) LLP v Barclays Bank Plc* [2014] EWHC 3049 (Ch), summary of legal principles found at paras 119 et seq, available: https://www.bailii.org/ew/cases/EWHC/Ch/2014/3049.html; note in *Douglas v Hello!*, the competing magazine, OK, also sought to rely on confidentiality.

[565] *Pollard v Photographic Company* (1888) 40 Ch D 345; *Creation Records v News Group Newspapers* [1997] EMLR – a scene was constructed for photography to create an album cover; the photographer took the pictures surreptitiously and despite security measures to prevent unauthorised photography.

[566] *Campbell*, para 51

[567] See e.g. *Ferdinand v MGN* [2011] EWHC 2454 (QB)

[568] *Murray v Big Pictures* [2008] EWCA Civ 446, available: https://www.bailii.org/ew/cases/EWCA/Civ/2008/446.html

[569] *Weller and Ors v Associated Newspapers* [2015] EWCA 1176

[570] *Campbell*; *Theakston v MGN* [2002] EWHC 137 (QB); *Richard v BBC* [2018] EWHC 1837 (Ch), available: https://www.judiciary.uk/wp-content/uploads/2018/07/cliff-richard-v-bbc-judgment.pdf.

In *Gulatti* (concerning the phone hacking scandal) it was accepted that misuse of information could arise as regards mode of acquisition of information as well as its communication[571] (as it would be intrusion). In *PJS* the Supreme Court noted that the repetition of known information could constitute with each repetition a further invasion of privacy, pointing out that a claim for misuse of private information is not solely concerned with 'secrets' but the level of intrusion and harassment the claimant will suffer. It also suggested that there is a difference between the level of intrusiveness depending on the level of intimate detail that is published; PJS concerned a kiss-and-tell story.[572] This reaffirms the difference between confidentiality and misuse of private information.[573]

Malicious falsehood was used (arguably stretched) in the pre-HRA case of *Kaye v Robertson* to try to deal with an outrageous invasion of privacy – where an actor in hospital was 'interviewed' and a newspaper claimed he had sold his story.[574] can be claimed by the publication of false words referring to the claimant (or the claimant's property or business). It is different from defamation in that there is no need to prove damage to reputation, but damages are usually lower than in a defamation action. A second different concerns the single meaning rule which applies in relation to defamation[575]; it does not apply here, so a claim can be made in respect of any meaning.[576] A malicious falsehood claim can survive the death of either party.[577] The Scots have an equivalent action.[578]

The old case of *Wilkinson v Downton*[579] provided the basis for a ***tort of intentionally causing harm***. This was considered recently in *Rhodes*[580], which might limit its usefulness - at least in cases of publication. Rhodes had written an autobiography detailing the abuse he had suffered as a child; his ex-wife was concerned that reading the book might lead to psychological damage being suffered by their child. The Court of Appeal held that this constituted intentionally causing harm, but this was over-turned by the Supreme Court. This confirmed there are three elements to be shown: a conduct element, a mental element and a consequence element. The conduct element required words or conduct directed towards the claimant for which there was no justification or reasonable excuse. Here the conduct (publishing a book) was not conduct directed towards the claimant. Further, freedom to report the truth enjoys a very high level of protection. The Supreme Court opined that it would be difficult to envisage any circumstances in which speech which was not deceptive, threatening or possibly abusive could give rise to liability in tort for willful infringement of another's right to personal safety.

A recent Court of Appeal judgment[581], over-turning the first instance decision held that being over-looked did not fall within the scope of the ***tort of private nuisance***. The case concerned the viewing gallery built at the Tate which allowed visitors to look into some near-by flats.

---

[571] *Gulatti v MGN* [2015] EWCA Civ 1291, available: https://www.judiciary.uk/wp-content/uploads/2015/12/representative-claimants-v-mgn.pdf
[572] *PJS* might have a significant impact on this genre of journalism; it is far from certain that *Ali & Anor v Channel 5 Broadcasting Ltd* [2019] EWCA Civ 677 (see further below) will be as critical for fly-on-the-wall "documentaries".
[573] *Google Inc v Vidal-Hall and ors* [2015] EWCA Civ 311, available: http://www.bailii.org/ew/cases/EWCA/Civ/2015/311.html
[574] *Kaye v Robertson* [1991] FSR 62 CA
[575] The principles have been summarised recently in *Koutsogiannis v Random House Group* [2019] EWHC 48, para [12], available: https://www.bailii.org/ew/cases/EWHC/QB/2019/48.html
[576] *Ajinomot Sweeteners Europe SAS v Asda Stores Ltd* [2010] EWCA 609
[577] *Hatchard v Mege* (1887) 18 QBD 771
[578] See e.g. *Barratt International Resorts Limited v Barratt Owners' Group* [2002] ScotCS 318
[579] *Wilkinson v Downton* [1897] 2 QB 57
[580] *Rhodes v OPO* (by his litigation friend BHM) [2015] UKSC 32
[581] *Fearn and Ors v The Board of Trustees of the Tate Gallery* [2020] EWCA Civ 104

The role of providers and distributors

The provisions of the e-Commerce Directive are implemented principally through the The Electronic Commerce (EC Directive) Regulations 2002.[582] Regulation 19 provides the hosting immunity. The relationship between giving notice and intermediaries/platforms acquiring such knowledge is found in Regulation 22:

> In determining whether a service provider has actual knowledge … a court shall take into account all matters which appear to it in the particular circumstances to be relevant and, among other things, shall have regard to–
>
> (a) whether a service provider has received a notice through a means of contact made available in accordance with regulation 6(1)(c), and
>
> (b) the extent to which any notice includes–
>
> (i) the full name and address of the sender of the notice
> (ii) details of the location of the information in question; and
> (iii) details of the unlawful nature of the activity or information in question.

The question of whether Facebook had knowledge was concerned in the Northern Irish Court of Appeal in *CG*.[583] The information complained of on the face of it was not particularly sensitive, there had been threats of violence against the claimant, which triggered a reasonable expectation of privacy. The question then was whether the hosting exception in Regulation 19 applied. A previous case had involved similar content and context but different parties. The Court of Appeal held that the claimant could not rely on this case to argue that Facebook had constructive knowledge (but partly because it did not involve a privacy claim). Facebook did have knowledge in relation to one of pthe pages complained of on the basis of a letter in which the claimant's solicitors complained of the identification of the general area in which he was living and referred to the police having warned him that his life was under threat from paramilitaries. Facebook was on notice of the risk to CG and failed to act expeditiously to take down the information. Note a claimant does not have to use the online form specified by the platform operator.

CG is one of a number of cases in Northern Ireland testing out the scope of knowledge for the purposes of immunity;[584] most seem to settle at an early stage. There have been comparatively few recent English cases.[585]

---

[582]Available: The Electronic Commerce (EC Directive) Regulations 2002. Note a number of other statutes contain analogous provisions.
[583]*CG v Facebook Ireland* [2016] NICA 54
[584]See also *MM v BC, RS and Facebook Ireland* [2019] NIMaster 5; *J20 v Facebook Ireland* [2016] NIQB 98
[585]See e.g. *Tamiz v Google* [2013] EWCA Civ 68, [2012] EWHC 449 (QB); *Bunt v Tilley* [2006] EWHC 407 (QB); *Kaschke v Gray* [2010] EWHC 690 (QB); *Davison v Habeeb and Others* [2011] EWHC 3031 (QB).

In addition to immunity rules generally (implementing the e-Commerce Directive Art 12-14), there is a defence available in re defamation under s. 1 Defamation Act 1996 where the defendant does not have knowledge that or have reason to believe that a statement is defamatory and provided that it was not the author, editor or publisher of the statement and took reasonable care.

Further, the Defamation Act 2013 seems to have tilted the balance in favour of platforms. It amended the English law of defamation to provide a single publication rule. Under the previous law an online article was considered to have been re-published every time it was accessed by a reader. Section 8 Defamation Act 2013 provides that the limitation period of 12 months runs from the date of first publication to the public, notwithstanding subsequent publication of a statement which is substantially the same. This section will not apply where the publication is by a different person or the subsequent publication is materially different in manner from the first (section 8(4)). There has not been any judicial consideration of this provision.

Section 5 relates to online libel and will, in certain circumstances, provide website operators with complete immunity. Section 5(2) provides that it will be a defence for an operator of a website to show that it was not they who 'posted' the statement on the website. Under section 5(3), the defence will be defeated if all three of the following conditions apply:-

(a) It was not possible for the claimant to identify the poster of the statement,

(b) The claimant gave the operator notice of their complaint in relation to the statement, and

(c) The operator failed to respond to the notice in accordance with any provisions contained in regulations.

Identification is only possible where the claimant has sufficient information to bring proceedings against the person in question (section 5(4)). According to the Government the aim of s. 5 and the Defamation (Operators of Websites) Regulations 2013,[586] which set out the form of notice required from the Claimant and the relevant procedure that must be followed by the website operator if he/she/it wishes to utilise the section 5 defence, is 'to support freedom of expression' and to limit operator liability where the person who has posted it co-operates but wishes to stand by the material posted[587]. It is open to the website operator to ignore the availability of section 5 (and any notice served by a claimant) and defend any claim on other grounds (e.g. section 1 of the Defamation Act 1996 or Regulation 19 of the Electronic Commerce (EC Directive) Regulations 2002. The s. 5 route has not been much used, if at all. Some commentators noted that the language used in the act was, even at the time is was enacted, old-fashioned and that there might be some dispute as to what an 'operator of a website' might mean (e.g does it cover apps, or an access service). Litigation on this point has not materialised as yet.

Section 10 states that the Court does not have jurisdiction to hear a defamation claim against a person who was not the author, editor or publisher of the statement complained of unless satisfied that it is not

[586]The Defamation (Operators of Websites) Regulations 2013 (SI 2013/3028), available: http://www.legislation.gov.uk/ukdsi/2013/9780111104620
[587]https://hansard.parliament.uk/Lords/2013-11-19/debates/13111956000153/Defamation(OperatorsOfWebsites)Regulations2013

reasonably practicable for an action to be brought against the author, editor or publisher (e.g. they were unknown).[588] It is unclear when the reasonably practicable test would be satisfied. The acceptability of suing persons unknown has been established for some time and it is possible to apply (via a *Norwich Pharmacal* order) for the identity of a person to be made known. This means that targetting platforms as secondary publishers will only be acceptable in limited circumstances and seems to provide protection to the platform irrespective of whether the platform complied with requirements under s. 5 Defamation Act 2013. Note s. 10 does not apply just to the digital environment.

Section 13 provides that where the court gives judgment for a claimant, it may order the operator of a website to remove the statement or any person who was not the author, editor, or publisher of the statement to stop distributing, selling or exhibiting it. This has not been used; it seems that some intermediaries remove content under community standards processes once aware of a adverse ruling in relation to content. Section 12 allows the possibility for defendants to be order to publish an agreed form description of the judgment (which has rarely been used).

Drones are regulated from the perspective of aviation safety, and there are restrictions on flying drones near airfields. The Drone Code nonetheless suggests never flying closer that 150m to built up areas, or fly directly over them, or directly over a crowd. Commercial operators were subject to more restrictions, but the rules are in the process of changing[589] to align with EU standards; registration is now required. Operators of drones must comply with the Data Protection Act.[590]

There are no specific rules regarding the sale of spycams or other tracking tools; the obligation for compliance will fall on the purchaser/user though the ICO has a specific code relating to CCTV.[591] Note that under the Protection of Freedom Act 2012, the role of Surveillance Camera Commissioner was introduced (though it is not clear what the status of the role is going forward[592]), as well as a specific code on surveillance cameras.[593] The Code is mandatory only for some public bodies; respect for the code for private actors is good practice only. Some uses may fall foul of the criminal law (e.g the stalking offences under the PHA), as well as giving rise to potential causes of action under the civil law. In addition to data protection obligations, the UK government has produced a voluntary Code of Practice for consumer IoT devices[594]; it is proposing to strengthen the obligations which may introduce liability beyond the user. It does not address other privacy conerns such as always on smart devices recording people.

At the time of the phone-hacking scandal obtaining unauthorised access to others' phone calls and messages was regulated by the Regulation of Investigatory Powers Act 2000 (RIPA) – this was a criminal offence unless carried out by the police or intelligence services under warrant. The Investigatory Powers Act 2016[595] now provides:

3 (1)A person commits an offence if—

[588]Discussed in *Brett Wilson LLP v Persons Unknown* [2015] EWHC 2628 (QB)
[589]See also bill currently before Parliament: https://services.parliament.uk/Bills/2019-21/airtrafficmanagementandunmannedaircraft.html
[590]https://ico.org.uk/your-data-matters/drones/
[591]https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
[592]https://videosurveillance.blog.gov.uk/2020/02/19/a-farewell-looking-back-to-the-future-through-the-camera-lens-part-1/
[593]https://www.gov.uk/government/publications/surveillance-camera-code-of-practice
[594]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf
[595]https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

(a) the person intentionally intercepts a communication in the course of its transmission by means of–

(i) a public telecommunication system,

(ii) a private telecommunication system, or

(iii) a public postal service,

(b) the interception is carried out in the United Kingdom, and

(c) the person does not have lawful authority to carry out the interception.

The 2016 act carries greater emphasis on the need to protect privacy than its predecessor. Equipment interference (hacking) is precluded by the Computer Misuse Act 1990[596]. 'Directed surveillance' and 'intrusive surveillance' are dealt with by RIPA; state activity in this regard is controlled with a code of practice giving further details[597]; the act seems to cover only surveillance carried out by state authorities.

[596] https://www.legislation.gov.uk/ukpga/1990/18/contents

[597] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

Part 2: Protection of privacy and data in horizontal relations

Data protection legislation

Relevant articles and rationale

One particular peculiarity of the Data Protection Act 2018[598] is the introduction of the Age Appropriate Design Code by virtue of s 123. It is apparently limited to explaining how the GDPR applies to children (as per Recital 38 GDPR), but the "clarifications" might be quite far-reaching and it is a statutory code that must be complied with. The provision was introduced as an amendment to the Data Protection Bill and it had cross party support. It applies to providers of information society services that are likely to be accessed by children. This includes applications, websites, search engines, community environments, programs, games, and connected toys or devices. The Code takes as its starting point the UN Convention on the Rights of the Child to derive 15 standards of age-appropriate design which include strict privacy default settings. Although the UK opted for an age of digital consent of 13, the Age Appropriate Design Code views children as those under 18. Following the code coming into force, there will be a 12-month transition period to allow organizations to implement the standards. The ICO expects the transition period to end by autumn 2021. While the central focus of this provision (introduced by Baroness Kidron as an amendment to the data protection bill) was the protection of children,[599] there was also a broader concern about manipulation of individuals generally by platform design.

In addition to the right of action given to individuals as required by the GDPR, the DPA introduces a number of criminal penalties to support the taking seriously of the obligations under the act by private actors: unlawful obtaining of personal information[600] ("blagging", an offence which was introduced under the DPA98[601] and was discussed as part of the Leveson Inquiry[602]); re-identification of de-identified personal data[603]; and destroying or altering information so as to avoid responding to a subject access request.[604]

Case law

A claim under DPA can be brought alongside a defamation claim or misuse of private information action – or indeed any of the other private actions.[605]

In Lloyd v Google sought to bring a class action (an 'opt out' claim on behalf over 4 million plus Apple iPhone users) alleging Google had secretly tracked some of their internet activity, for commercial purposes, between August 2011 and February 2012. To serve out of the jurisdiction he had to show he had a reasonable chance of success which the High Court held he did not for two reasons: none of the people had suffered damage under s 13 DPA98; and the members of the 'class' did not share the same interest.

[598]https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[599]https://hansard.parliament.uk/lords/2017-12-11/debates/154E7186-2803-46F1-BE15-36387D09B1C3/DataProtectionBill(HL)
[600]S 170 DPA18
[601]For an example, see here:https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/06/former-claims-company-manager-fined-2-000-over-blagging-calls-to-obtain-personal-data/
[602]Concerns remain: https://hansard.parliament.uk/Commons/2018-03-07/debates/0807762B-26A4-4BAA-9361-4F7DDB6B0DF8/BlaggingLevesonInquiry
[603]S. 171 DPA18
[604]S. 173 DPA18
[605]*Hicham v Elaph Publishing* [2017] EWCA Civ 29

The Court of Appeal overturned this decision.606 In so doing, the Court of Appeal accepted that the claimants suffered damage through the loss of control of their data, referring also to Rec 85 GDPR. If the browser generated information (BGI) had a commercial value, a person's control of those data should also have a value; it did not require proof of loss. This also allowed the Court to find that the claimants all had the same interest: they are all victims of the same alleged wrong, and have all sustained the same loss, namely loss of control over their BGI. Although the action was brought under the 1998 act, the Court was at pains to emphasise that its reasoning applied under the DPA18/GDPR. The Supreme Court has granted permission to appeal; the case is pending.

The Court of Appeal judgment in Lloyd has been regarded as ground-breaking in terms of its broad interpretation of the 'same interest' and making it much easier for claimants to bring class actions, even those requiring service out of the jurisdiction. There are a couple more class actions now starting, following on from findings from the ICO of breach of data protection law based on the 'loss of control' argument found in Lloyd. Equifax received the then maximum fine under the DPA98, but group litigation is now going forward; a group litigation order has also been issued by the High Court in relation to litigation against British Airways. Some commentators have questioned whether this signals a change in the perception of what litigation is supposed to do: traditionally litigation was about obtaining compensation (for the loss caused by the breach of contract or the tort by putting them in the position they would have been in had the breach and resulting loss not occurred), not -on the whole - censuring firms. Yet certainly in Lloyd the claimants were claiming no pecuniary loss. It is possible that the courts might adopt an approach referred to as 'user damages'. In One-Step,607 a case which did not involve data protection but misuse of confidential information (of a business), the Supreme Court held that damages can be awarded where a person "takes something for nothing…the owner is entitled to require payment".608

A case regarding the vicarious liability for the infractions of an employee is currently before the Supreme Court.609 In Morrisons, a senior IT internal auditor leaked payroll information of approximately 100,000 employees. He was convicted for various criminal offences. The employees brought civil actions (using a group litigation order) against Morrisons. The Court of appeal found that the DPA does not exclude the possibility of vicarious liability. The test requires the court to consider two matters; first, what 'field of activities' have been entrusted by the employer to the employee; and second, whether there was sufficient connection between the position in which he was employed and his wrongful conduct to make it right for the employer to be held liable. Counsel for Morrisons argued the second test was not satisfied because the leak was done at the employee's own home, using his computer; further the employee's aim was to harm Morrisons. Nonetheless the Court of Appeal rejected these arguments and found Morrison's liable.

Actions by the supervisory authority

606 *Lloyd v Google* [2019] EWCA Civ 1599
607 *One-Step v Morris-Garner [2018] UKSC 20, available: https://www.supremecourt.uk/cases/uksc-2016-0086.html*
608 For a summary of the context of the case see: http://ukscblog.com/case-comment-morris-garner-v-one-step-support-ltd-2018-uksc-20/
609 https://www.supremecourt.uk/cases/uksc-2018-0213.html

The Data Protection Act to a large part concerns horizontal relations; the general guidance on the act (and the GDPR) would therefore fall within this category. The ICO does not however pay particular attention to this aspect. The guidance is available on the ICO website, as are details of enforcement actions.[610]

One of the most famous series of cases of recent years has been the phone hacking. These cases have been brought however by the affected individuals rather than by the ICO. At the DCMS Select Committee into Press Standards, privacy and libel (2009), the then Information Commissioner said that his predecessor did not have the resources to prioritise the issue and that therefore it would not have been good regulation. The ICO subsequently, and as suggested by the Leveson Inquiry, provided guidance on data protection and journalism. The DPA18 requires the ICO to produce a code of practice on the use of personal data in journalism, and also to carry out periodic reviews on compliance.

The ICO's resources have been increased since the entry into force of the GDPR/DPA18, though there have been some questions in the practitioner sector as to how well the ICO is progressing day-to-day complaints.[611] The current Information Commissioner has prioritised the investigation into Cambridge Analytica (which led to a fine on Facebook as well as extra-territorial enforcement), interactive advertising[612] and political advertising.

One interesting development was the use by the ICO of the Computer Misuse Act (rather than the DPA) to penalise an individual who used a co-worker's log-in details to illicitly gain access to customer data.[613] The ICO has also been consulting on the possibility of use the Proceeds of Crime Act powers in relation to those convicted of a data protection offence.[614]

Significance in practice

In practice (as opposed to academia) the focus has been on the development of class actions and the courts' approach to 'loss of control' as the basis for liability. There has also been a certain amount of litigation in relation to data subject access requests (DSARS), and in particular their use as part of litigation, though these relate to DPA98. The more high profile investigations have yet to have had much impact – though the nature of the higher profile matters is that they take time.

[610] https://ico.org.uk/
[611] See for example, https://2040infolawblog.com/ – though this blog never gives statistics or formal analysis.
[612] Summary of work here: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/blog-adtech-the-reform-of-real-time-bidding-has-started/
[613] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/six-month-prison-sentence-for-motor-industry-employee-in-first-ico-computer-misuse-act-prosecution/
[614] https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-on-the-application-for-powers-under-the-poca/

Administrative, anti-trust and consumer protection law

Relevant articles and rationale

The ICO has responsibility for enforcing data protection rules. In addition, Ofcom has some responsibilities for adjudicating on complaints about invasions of privacy in the context of broadcasting by virtue of sections 3(2)(f) and 326 of the Communications Act 2003, sections 107(1) and 130 of the Broadcasting Act 1996 (as amended). Ofcom has incorporated rules into its Content Code[615] that, rather than being concerned with what viewers see, deal with how broadcasters treat the individuals or organisations directly affected by programmes. This is a reformulation of powers exercised by predecessor regulators in this field.[616] Note that these provisions deal with fairness as well as privacy; these elements are dealt with separately from the 'standards' rules, which include rules regarding harmful stereotyping too. Rule 8.4 contains provisions about surreptitious filming and there have been a number of Ofcom decisions on this point.

Ofcom is also consulting on a further change to its Code in relation to the protection of individuals taking part in television shows (especially reality tv).[617] This follows increased public concern, including a Parliamentary committee inquiry[618], into how participants are treated and concern for their mental health and well-being.

Anti-trust and consumer protection law

The Competition and Markets Authority is entrusted with competition law enforcement and consumer protection. There are no specific provisions dealing with privacy in this context.

Nonetheless there have been concerns around digital dominance and the use of data- specifically profiling. This has engaged the CMA's competition powers rather than consumer law powers – though the CMA has called for more enforcement powers in these areas. Specifically, the Chairman of the CMA (Tyrie) wrote to the Secretary of State for Business, Energy and Industrial Strategy (BEIS) to suggest a new statutory duty on the CMA and on the courts to treat the interests of consumers and their protection from detriment as paramount as well as improving the investigatory and information -gathering powers.

In 2018 the then Chancellor set up the Digital Competition Expert Panel chaired by Prof. Furman; its report[619] is usually referred to as the Furman Report. It investigated whether traditional competition law was sufficient to deal with the digital environment. It proposed reform and specified six strategic recommendations, which were accepted by the Government in the recent budget. Specifically a new dedicated digital markets unit and a 'cross-regulator' taskforce. This unit will set a code of conduct for players with "strategic market status" and pursue data interoperability including access to non-personal and anonymised data (presumably whether the individuals concerned are happy with this or not). A report on the code of conduct is due to be published in Sept 2020.

---

[615]See here: https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code/section-eight-privacy
[616]For a background as to the pre-Communications Act system see:
https://publications.parliament.uk/pa/cm200203/cmselect/cmcumeds/458/458.pdf
[617]https://www.ofcom.org.uk/consultations-and-statements/category-2/protecting-tv-radio-participants
[618]https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/inquiries/parliament-2017/realitytv/
[619]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

The CMA (following on a number of investigations into digital markets) launched a digital markets strategy and in part responding to the Furman Report. One key step was the opening of a market study into online platforms and the sources of any market power, the way they collect and use personal data, and whether competition in digital advertising is producing good outcomes for consumers.[620] The CMA has published its interim report; the deadline for comments closed on 12 February 2020.

The Furman Review also suggested that there should be monitoring of developments in relation to machine learning algorithms and artificial intelligence by the government, the CMA and the Centre of Data Ethics and Innovation (CDEI), with a view to ensuring that developments do not lead to consumer detriment or anti-competitive activity. The CDEI has recently published a report on online targeting[621].

Case law

Ofcom's decisions are occasionally subject to judicial review – but such actions are very rare and the courts have tended to defer to the specialist regulator.[622] Ofcom's approach is based on case law on Articles 8 and 10.

Actions by supervisory authorities

For examples of surreptitious filming decisions see for example the complaints of unfair treatment and unwarranted infringement of privacy in relation a programme called 'The Lobby', which involved an undercover reporter.[623] By contrast to the recognition of public interest when politicians are involved, Ofcom has been prepared to find breach in the cases of private individuals.

One OFCOM ruling that shows enforcement of privacy was a ruling in relating to fly-on-the-wall reality tv (*Can't Pay? We'll Take it Away*) which dealt with High Court Enforcement Agents (HCEA).[624] The complained of programme contained footage from body worn cameras of the complainant inside her parents' house. Ofcom found a breach both in obtaining the footage and in its inclusion in the programme. A key factor was that the body worn cameras were provided by the film-maker; they were not there for evidential reasons or to protect the HCEAs. Some commentators have suggested that this decision shows Ofcom paying more respect to Article 8 rights than hitherto when balancing against Article 10: 3 previous decisions in relation to the series were not upheld, though each could be fact specific. The same series was the subject of an adverse judgment on the basis of misuse of private information in the courts in *Ali v Channel 5*, when the HCEAs were filmed trying to evict the applicants for non-payment of rent.[625]

[620]The inquiry page, including link to interim report, is here: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
[621]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/864167/CDEJ7836-Review-of-Online-Targeting-05022020.pdf
[622]See e.g. *Traveller Movement v BBC* [2015] EWHC 406 (Admin) and comment: E. Steyn 'Big Fat Gypsy Weddings get OFCOM (and High Court) approval' [2015] *Ent LR* 142
[623]Available: https://www.ofcom.org.uk/__data/assets/pdf_file/0033/106989/issue-338-broadcast-on-demand-bulletin.pdf
[624]For summaries of other Ofcom decisions in relation to this series see: https://www.nationalbailiffadvice.uk/ofcom-dcbl-complaints.html
[625]*Ali & Anor v Channel 5 Broadcasting Ltd* [2019] EWCA Civ 677

Significance in practice

Discussions relating to Ofcom have tended to focus on individual decisions[626]; the systems aspects were considered when the 2003 regime came in and that was mainly descriptive.[627] There has been some comment about Ofcom's changes to its approach to fines to increase the deterrent effect of the regime, which means that the size of the undertaking may be taken into account when setting the level of fine.[628]

Criminal law

Relevant articles and rationale

Criminal act	Relevant article(s)	Description
Defamation, slander and libel	N/A – civil law	
Surreptitious monitoring (visual, aural, electronic) (e.g. camera surveillance, eavesdropping, spyware)	Potentially stalking offences under ss 2A and 4A Protection from Harassment Act[629] s. 76 Serious Crime Act 2015[630]	No definition of stalking: s 2A(3) gives non-exhaustive list of examples: (d) monitoring the use by a person of the internet, email or any other form of electronic communication; (g) watching or spying on a person; also requires a course of conduct domestic abuse offence to capture coercive and controlling behaviour in intimate and familial relationships (which might not fall within PHA) – can include use of spyware
Harassment	Protection from Harassment Act s 2	a course of conduct; which amounts to harassment of another; and which the defendant knows, or ought to know amounts to harassment of another.

[626]See e.g. J. Agate 'Regulating fictionalised reality: Ofcom decision on murder drama' [2017] *Ent LR* 238; T. Iverson 'Sky handed paddle by Ofcom in Canoe Man privacy decision' [2013] *Ent LR* 257; J. Agate 'Privacy, children and reality TV: Ofcom ruling on C4 broadcast' [2018] *Ent LR* 17; C. Wenn 'Infringing privacy – Channel 5 gets the balance wrong in its depictions of gang violence' [2018] *Ent LR* 169

[627]J. Epworth 'Protecting your private life: the future of OFCOM privacy complaints' (2005) 10 *Comms L* 191.

[628]E. Steyn 'OFCOM's revised guidelines on fines – a new emphasis on deterrence' [2016] *Ent LR* 150.

[629] See CPS Guidance: https://www.cps.gov.uk/legal-guidance/stalking-and-harassment

[630] Statutory guidance available here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/482528/Controlling_or_coercive_behaviour_-_statutory_guidance.pdf

	s.1 (1A)	Harassment of more than one person to do or not do something
Location tracking	Not specifically address; could be covered by harassment rules[631] See also Serious Crime Act 2015	see above – could include software to track movements
Stalking	S 2A Protection from Harassment Act s 4A Protection from Harassment (re England); S. 39 Criminal Justice and Licensing (Scotland) Act 2010 (re Scotland) Northern Ireland has reviewed need for specific offences.[632]	Stalking stalking involving fear of violence/serious alarm/distress Racially or religiously aggravated stalking
Extortion (e.g. sextortion)	s. 33 Criminal Justice and Courts Act 2015; s 21 Theft Act	
Publication of sexual images (e.g. revenge porn)[633]	s. 33 Criminal Justice and Courts Act 2015[634] (this applies to England – see s 2 Abusive Behaviour and Sexual Harm (Scotland) Act 2016) Abusive Behaviour and Sexual Harm (Scotland) Act 2016.	*Disclosure of a private sexual photograph or film if the disclosure is made without the consent of the individual who appears in the photograph or film, and with the intention of causing that individual distress*[636] *[if no intent to cause distress then not within scope]*

[631]https://www.cps.gov.uk/north-west/news/man-sentenced-stalking-ex-girlfriend
[632]http://www.niassembly.gov.uk/assembly-business/committees/2016-2017/justice/inquiries--reviews/review-of-the-need-for-stalking-legislation-in-northern-ireland/
[633]The Law Commission is carrying out a review of the law in England and Wales: http://www.lawcom.gov.uk/project/taking-making-and-sharing-intimate-images-without-consent/; note also strategy against violence against women and girls (VAWG) also as part of social media guidance: https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media
[634]Discussed Appendix 1, Rook and Ward on Sexual Offences (5th ed), Supplement, for criticism see S. Pegg 'A matter of privacy or abuse? Revenge Porn in the Law' [2018] Crim LR 512
[636]CPS Guidance is here: https://www.cps.gov.uk/legal-guidance/revenge-pornography-guidelines-prosecuting-offence-disclosing-private-sexual

	Sexual Offences Act 2003 (amended by Voyeurism (Offences) Act 2019)[635] (previously dealt with common law outraging public decency) s. 1 Protection of Children Act 1978 s. 160(1) Criminal Justice Act 1998 s 15A Sexual Offences Act (inserted by s. 67 Serious Crime Act 2015)	*instances where the purpose of the behaviour is to obtain sexual gratification, or to cause humiliation, distress or alarm* *the taking, making, distribution, showing or possession with a view to distributing any indecent image of a child – this could include sexting possession of indecent photograph of a child*[637] *sexual communication with a child*[638] (grooming)
Publication of pictures of helpless people (e.g. filming traffic incidents)	See s. 127 Communications Act – no specific offence	See e.g. Mwaikambo, not reported[639]
Other,[640] namely:	s. 127 Communications Act s 1 Malicious Communications Act	sending a communication that is grossly offensive, indecent, obscene, menacing or false - sending a communication that is grossly offensive, indecent, obscene,

[635] Nb upskirting was already a criminal offence in Scotland
[637] Harm is described in R v Beaney [2004] EWCA Crim 449
[638] See guidance here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/604931/circular-commencement-s67-serious-crime-act-2015.pdf
[639] https://www.telegraph.co.uk/news/2017/06/16/man-jailed-sharing-photo-dead-grenfell-tower-fire-victim-facebook/; see discussion by L. Logan and A. Gozen 'Reporting on Sensitive Current Events' [2018] Ent LR 250
[640] See Law Commission Report on Abusive and Offensive Online Communications (2018), available: https://www.lawcom.gov.uk/abusive-and-offensive-online-communications/

	s. 1 Sexual Offences (Amendment) Act 1992 s. 66 Sexual Offences Act Note general public order offences (e.g Public Order Act 1986)	conveys a threat or is false, with intent to cause distress or anxiety[641] publishing the name of a complainant in re certain sexual offences exposure of genitals – realtime (e.g livestreaming) – nb intent to cause alarm or distress

Analysis of criminal law provisions

There is little in the way of direct privacy protection through the criminal law; the Law Commission notes some concerns about this[642]. The general background for criminal law as regards privacy and personality rights seems to have been (physical) sexual offences. These recognise the threats to personal autonomy/human dignity, though there is no overarching framework for these various offences and the motivations concerning the different offences have differed. The communications offences have also been used to deal with the abuse of communications technologies (though these are far from a perfect solution) or (depending on facts) PHA could be used instead – for example, in cases of serious 'doxing'. The data protection offences above could also be used, though they do not carry heavy penalties, which might be deemed inappropriate in severe cases.

Since the mid-1990's as regards the private sphere, it seems that there has been some recognition that behaviour that falls short of traditional physical assault have significant impacts on people (often women), as can be seen with the introduction of the PHA. This was originally introduced to target stalking. Concerns that the protections were inadequate led to the amendment of the PHA through the Protection of Freedoms Act. A subsequent private members bill (supported by the Government) more recently introduced a civil order - 'Stalking Protection Orders' - which will be applied for by the police which will apparently allow the police to tackle 'stranger stalking' sooner and more effectively (those stalked within the context of domestic abuse may be protected by Domestic Abuse Protection Orders). Although the Stalking Protection Orders are a civil law mechanism, breaches will trigger criminal sanctions. There is a more general strategy in the background: the Government's increased awareness of violence against women and girls (VAWG). A number of the general criminal offences may have a VAWG element – specifically stalking and harassment, as well as pornography and sexual offences. Indeed, the CPS guidance recognises that social media offences may have VAWG elements.[643]

[641] *Chambers v DPP* [2013] 1 WLR 1833; on s. 127 see J Rowbottom 'To rant, vent and converse: protecting low level digital speech' (2012) 71 CLJ 355; in Scotland see e.g. Rodgerson v Dunn [2016] HCJAC 12, noted C. M. Shead 'The Decision in Rodgerson v Dunn' [2016] SCL 255 and Sutherland (Adam) v HM Advocate [2017] HCJAC 22

[642] Law Commission, *Abusive and Offensive Online Communications*, para 10.28

[643] See https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media

The issue of revenge porn was tackled specifically through s. 33 Criminal Justice and Courts Act 2015 (and covers online and offline sharing) – prior to this the CPS had to use the communications offences (e.g. Malicious Communications Act) to tackle the problem, though this did not apply to all cases.

There have been concerns that the offence was not working effectively. One concern was that the lack of anonymity when a case went to court compounded the shame and distress already suffered by the victim – and that this led to complaints being withdrawn (it is categorised as a communications crime not a sex crime). This matter is under review by the Law Commission. There were also concerns about narrow definitions – for example, that the offence would not cover deep-fakes; it may not adequately protect those groups who have a stricter standard of modesty. In 2018 sentencing guidelines were introduced (covering stalking and harassment as well as revenge porn), with an aim to more severely punish those who repeatedly post material after is has been taken down, as well as those who deliberately set out to embarrass their victims.

Another specific development was the introduction of 'upskirting' offences through the Voyeurism Act 2019.[644] Prior to its introduction the criminal law only provide partial protection (common law offence of outraging public decency or s. 67 Sexual Offences Act 2003 and, for children, the Protection of Children Act); much depended on the facts of the case. The common law offence of outraging public decency has been used in a variety of contexts[645]- including in relation to upskirting[646], but also physically abusing and urinating on a woman dying in the street[647]. The offence requires that the complained of act be public, which means that more than one person be there who could have seen the act. It was this aspect that has given rise to difficulties for those claiming upskirting; this photography is often carried out surreptitiously; it is an open question whether multiple persons viewing the output online would satisfy this test.[648]

The Voyeurism Act aims to solve this problem. Itcreates 2 new offences and amends the Sexual Offences Act. The offence aims to be technology neutral (it refers to "equipment"[649]); the threshold is that the behaviour has the purpose of obtaining sexual gratification or causing humiliation, distress or alarm – seemingly covering those who claim to take such images 'for a laugh'. Some questions have been raised as to whether the definitions are too narrow, to the extent that the offence might not cover 'down-blousing'. Upskirting had already been a criminal offence in Scotland, and it has been suggested that the definitions there are more effective.[650] It is not an offence in Northern Ireland, though there has been a review of the law[651]. Another advantage of the specific offence is that it will be characterised as a sexual offence thereby granting victims anonymity.

Another gap in the general legislation concerned the grooming of children. This led to the introduction of a specific offence of sexual communication with a child – s. 15A Sexual Offences 2003. Note that in theory the general communications offences – s. 127 Communications Act and the Malicious Communications Act

[644]For a critique see A. A. Gillespie 'Tackling Voyeurism: is the Voyeurism (Offences) Act 2019 a wasted opportunity?' (2019) 82 MLR 1107
[645]See generally Law Commission, *Simplification of Criminal Law: Public Nuisance and Outraging Public Decency* (2015) Law Com No 358.
[646]e.g. *R v Hamilton* [2007] EWCA Crim 2062
[647]*R v Anderson* [2005] EWCA Crim 3
[648]Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (2018) Law Com 381 (HC 1682), paras 6.120-6.137
[649]S. 68 Sexual Offences Act 2003 (as amended)
[650] s. 3 Abusive Behaviour and Sexual harm (scotland) Act
[651]Sir John Gillens, *Gillens Review: Report into the Law and Procedures in Serious Sexual Offences in Northern Ireland* (9 May 2019).

- could have covered this form of communication, but grooming messages tend not to be shocking or offensive as the would-be abuser seeks to gain trust. The new offence covers both online and offline communication. It is similar to an offence introduced in Scotland in 2010. Again, it seeks to be technology neutral: the communication could be written, verbal or pictorial and made in person, by phone, internet or by any other means - such as via a gaming system. In addition to the prohibition itself, a civil preventative order was introduced, the Risk of Sexual Harm Order. It will prohibit adults from engaging in inappropriate behaviour (eg sexual conversations) with children.

The two communications offences (s. 127 Communications Act and the Malicious Communications Act) have been used as catch-all provisions prior to the enactment of specific provisions. These could therefore be used to protect privacy (including human dignity). For example, after the Grenfell Tower disaster a man took photographs of body bags, including one that was open, and posted them. He was found guilty of an offence under s. 127. Many of the s. 127 cases have involved hate speech.[652]

Case law

A recent issue concerns the practice of filming sex without the consent of your partner. A man sought to have two voyeurism charges dismissed in relation to his filming sex with prostitutes. The voyeurism offence does not just require consent but also an expectation of privacy. The Court of Appeal dismissed the argument.[653] Interestingly, the Court had allowed the intervention of a woman who was seeking to review judicially the CPS for its failure to bring charges against a man who allegedly raped her and filmed her while she was undressed and asleep in a hotel bedroom. Following the court of appeal decision the CPS reversed its policy.[654]

Actions by the public prosecution, police or supervisory authorities

Relevant guidance has been linked in footnotes to the relevant statutory provision. In general, the Guidance is that of the Crown Prosecution Service (CPS), but there is some statutory guidance.

One current issue is the requirement that victims of rape have to hand their mobile phones to the police for examination leading to concerns that the victims are being treated like suspects and adds to the invasiveness.

The Sentencing Council has highlighted the harm inherent in voyeurism due to the intrusion into the victims privacy; it will be more serious if images are shared. There have been some criticisms of the sentencing guidelines in relation to voyeurism.

Significance in practice

There are some news suggestions that the number of prosecutions of offences such as revenge porn are low[655]; this may be due to a lack of anonymity. The reliance on the general

[652]Supra and also Law Commission Report (HC 1682) para 5.74 et seq
[653]Not yet reported; summary here: https://medium.com/@TheICLR/weekly-notes-legal-news-from-iclr-10-february-2020-6a91cdceff65
[654]https://www.centreforwomensjustice.org.uk/news/2020/1/28/cps-concede-judicial-review-in-case-brought-by-emily-hunt-following-last-minute-intervention-at-the-court-of-appeal
[655]J. Ledward and J. Agate '"revenge Porn" and s. 33: the story so far' [2017] Ent LR 40

communications offences as catchalls has two weaknesses: that to some extent the protection covered will vary depending on the facts; also that the use of s. 127 Communications Act and the Malicious Communications Act may not fully represent the seriousness of the intrusion.[656]The Law Commission has noted that the police may not fully understand these offences. Some concerns have been expressed that the sexual offences rules will mean that teenagers engaging in texting risk being charged with child pornography offences.[657]

Civil and commercial law

Relevant articles and rationale

The Copyright Designs and Patents Act (CDPA) may provide a vehicle whereby an individual can control use of private documents and photographs. Copyright attaches to a photograph and would protect a document such as a diary or private letters and, in principle, texts.[658] There are of course 'fair use' defences and freedom of expression is sometimes used to support try to support a broad interpretation of them.[659] Note, usually the owner of the copyright is the creator of the work not the subject of the photograph. Section 85 CDPA gives the right to an individual who commissions the taking of a photograph or the making of a film for private purposes to prevent them being made public.

The tort of ***passing off*** will only protect an individual's name or image if it is shown that these have been used in trade and attract goodwill, so will only protect a limited category of persons (those generating goodwill).[660] Passing off probably fails to address the real complaint of a celebrity, which is to prevent the unauthorised use of his persona. Moreover, the courts have not shown much enthusiasm for stopping defendants which were doing nothing more than 'catering for a popular demand among teenagers for effigies of their idols'[661]. In *Irvine*, the courts appeared to distinguish between merchandising and endorsement.[662] So, use of a celebrity's image on a web page in conjunction with commercial branding and goods offered for sale may create a false inference that the celebrity "recommends" the offered goods. In the 2013 *Rihanna case*, involving the use of the pop-star's image on a t-shirt for sale in the high street without her permission, although she won on the facts, the court made it clear that English law did not provide a free standing general right by a famous person (or anyone else) to control the reproduction of

[656]For a discussion of revenge porn prior to the enactment of the specific provision see S Pegg 'A matter of privacy or abuse? Revenge Porn and he law' [2018] Criminal Law Review 512
[657]R Arthur 'Consensual sexting and youth criminal records' [2018] Crim LR 381; c.f. C. Kennedy and A Phippen 'Sexting and sexting behaviour – "Oh you're all children, children do silly things. You'll be fine. Get over it!"' [2017] Ent LR 191
[658]*Associated Newspapers Ltd v HRH Prince of Wales* [2006] EWCA Civ 1776; see also the claim of the Duchess of Sussex against the publication by the press of letters written by her to her father includes a copyright aspect in addition to misuse of private information and data protection: https://sussexofficial.uk/?fbclid=IwAR1g05MOIL1IREeOPiuaw-visto_AVXVnSGte_mPUQTlS9JO3IINn_17QLQ.
[659]*Ashdown v Telegraph Group Ltd* [2001] EWCA Civ 1142
[660]Note also trading standards rules in relation to false celebrity claims about endorsements: Consumer Protection from Unfair Trading Regulations 2008 (SI 2008/1277)
[661]*Lyngstrad v Annabas Products* [1977] FSR 62 in re paraphernalia bearing the name and image of ABBA; see similarly in re sticker so fhte Spice Girls: *Halliwell v Panini SpA*, 6 June 1997.
[662]*Irvine v Talksport Ltd* [2003] EWCA Civ 423 which concerned racing driver Eddie Irvine in respect of the use of a photograph of himself holding a Talksport branded radio (this item had been added to the photograph) on a brochure advertising the station.

their image.[663] Protection is limited to the living. The need to rely on similar doctrines is also found in Scotland.[664] Guernsey has, however, introduced registered image rights.[665]

Some celebrities have registered their name/image/signature as trademarks (e.g.David Beckham), though the trademarks may be difficult to enforce. There is a risk that the use of the name or likeness would be deemed descriptive and so not be considered trademark use.

The code of practice underpinning the advertising regime (CAP Code) states that permission must be obtained by advertisers before a celebrity is referred to in an advert. The CAP Code also extends to online platforms.

Intermediary liability and duty of care for information society services

See section 3; note the UK has not transposed the text of Article 15 e-Commerce Directive.

The Online Harms White Paper proposed that some intermediaries (quite broadly defined) should be subject to a statutory duty of care (and a duty of care has a particular legal meaning in the UK different from this report's definition) to prevent certain forms of harm to users arising. Typically a duty of care requires reasonable care in relation to harm that is foreseeable; this ties back to the doctrine of negligence in tort. A statutory duty operates to specify some elements of the cause of action that would otherwise be determined by the case law (usually because the case law is problematic). The precise nature of the harms has not yet been identified. As a further step away from the tortious action, the statutory duty of care is to be enforced by a regulator and not through private, civil action.

Note that this is not intended to be content regulation but rather a systemic approach, requiring platform operators to undertake a risk assessment as to the likelihood of harms arising from the service offered, including harms arising from particular features and tools provided. The technical obligations arising from this overarching duty is to be filled in by a regulator (currently envisaged to be Ofcom), perhaps in consultation with a technical advisory board. This could be said to be a 'safety by design' approach but to include transparency requirements as well as sufficiently effective complaints mechanisms. While the precise form of the regulation has yet to be finalised, it is unlikely that upload filtering would be required (save perhaps in the context of identified child pornography – a recent report called for upload screening[666]). This approach to regulation also leaves untouched the existing causes of action as against the content itself (and the person posting it); it also does not remove immunity for that third party content. How the two regimes would inter-relate in practice it is difficult to predict given the current lack of detail.

It is clear that should an individual have obtained a court order for content removal, a platform operator should comply with it.

---

[663] *Fenty & Ors v Arcadia Group Brands Ltd (t/a Topshop) & Anor [2015] EWCA Civ 3 (available: https://www.judiciary.uk/wp-content/uploads/2015/01/fenty-others-v-arcadia-others1.pdf); [2013] EWHC 2310 (Ch), available: https://www.5rb.com/wp-content/uploads/2013/07/Robyn-Rihanna-Fenty-v-Arcadia.pdf*

[664] A summary can be seen in G Black, "Publicity and image rights in Scots law" (2010) 14 *Edinburgh Law Review* 364

[665] Image Rights (Bailiwick of Guernsey) Ordinance 2012 (Guernsey)

[666] The Independent Inquiry into Child Sexual Abuse (IICSA), Internet Investigation Report (March, 2020), available: https://www.iicsa.org.uk/publications/investigation/internet

Requirements in technology

None that I am aware of (beyond privacy by design and security by design). Note that the government is proposing to regulate IoT device security, which might provide protection against some forms of privacy intrusion but it is not primarily aimed at privacy protection.

Part 3: Mechanisms other than legislation

Non-legal mechanisms

Awareness

Schools are required to teach digital literacy and some groups/private actors have provided materials to support that. The UK Council for Internet Safety has developed a framework "Education for a Connected World" to form a basis for this.[667] Ofcom also has statutory duties in relation media literacy and has carried out significant research into the area, including adults' media literacy as well as children's.[668] The development of media literacy is also part of the Online Harms White Paper strategy. The government has also developed policy with regards to adults' essential digital skills which includes being safe online.[669]

The Revenge Porn Helpline shares sources of information to help victims of revenge porn.[670]

Self-regulation

The only self-regulatory mechanism of which I am aware is the press self regulation system. Following the phone hacking scandal a review was set up: the Leveson Inquiry. Following this the Press Recognition Panel (PRP) was established to approve the independence of any press self-regulatory body that chose to apply. One such has been approved: IMPRESS. Engagement with this system is not compulsory and the main press publishers have not engaged, setting up instead their own regulatory body IPSO which in the view of the PRP would not meets its criteria. Some press outlets do not subscribe to any regulatory body. The difficulty with the post-Leveson system is that some essential elements (cost benefits in case of trial) which would have incentivised publishers to comply with the system were enacted but not brought into force.

Manufacturers of listening devices and the like do not appear to subscribe to any particular codes of conduct.

[667] https://www.gov.uk/government/publications/education-for-a-connected-world
[668] https://www.ofcom.org.uk/research-and-data/media-literacy-research
[669] https://www.gov.uk/government/publications/essential-digital-skills-framework
[670] https://revengepornhelpline.org.uk/other-support/

17 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).[671] 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.

[671] 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.

18 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.

Over Considerati
Considerati is het juridisch en public affairs adviesbureau voor de digitale wereld, met kantoren in Amsterdam en Den Haag. Wij helpen organisaties maatschappelijk verantwoord te innoveren met digitale technologie en data. Dit doen we met drie gespecialiseerde teams:

Legal: voor een datastrategie die compliant is met privacyregelgeving
Responsible Tech: voor een ethisch kompas bij innoveren met data en algoritme
Public Affairs: voor maatschappelijk en politiek draagvlak voor innovaties

En dit doen we al meer dan 15 jaar voor zowel grote bedrijven en overheden als groeiende organisaties.

Neem contact met ons op via **info@considerati.com** of bel naar 020 73 70 069

Over het Tilburg Institute voor Law, Technology en Society
Het Tilburg Institute voor Law, Technology en Society is een multidisciplinair onderzoeksinstituut dat zich bezighoudt met vraagstukken betreffende de interactie tussen recht, technologie en maatschappij en hoe deze factoren elkaar vormen en beïnvloeden.

Als u meer wilt weten over het instituut dan kunt u deze informatie vinden op onze Engelstalige website. De informatie is alleen beschikbaar in het Engels gezien de internationale samenstelling van onze onderzoeksgroep. Daarnaast zijn wij gericht op het verdiepen en verbreden van ons netwerk door het betrekken van verschillende achtergronden, disciplines, culturen en landen bij ons onderzoekswerk.

Voor meer informatie kunt u ook kijken op: https://www.tilburguniversity.edu/nl/onderzoek/instituten-en-researchgroepen/tilt