

PELS RIJCKEN



Advisering aan de VNG inzake de gewenste beperking van het gebruik van slimme deurbelcamera's

Pels Rijcken en Highberg
19 december 2025



Inhoudsopgave

1. Inleiding	p. 3
2. Vraagstelling rapport	p. 4
3. Managementsamenvatting	p. 4
4. In hoeverre is het op grond van de AVG voor burgers en bedrijven toegestaan om gebruik te maken van slimme deurbelcamera's die mede zijn gericht op de openbare weg ter bescherming van zichzelf en hun eigendommen?	p. 8
5. Hoe verhoudt artikel 6, eerste lid, aanhef en onder f, AVG zich tot de grondrechten van passanten, in het bijzonder het recht op privacy dat wordt gewaarborgd door artikel 8 EVRM?	p. 15
6. In hoeverre bestaat er aan de zijde van de gemeente juridische ruimte om het gebruik van slimme deurbelcamera's die een deel van de openbare weg filmen, bij gemeentelijke verordening (APV) te reguleren?	p. 17
7. Wat is de reikwijdte van de gemeentelijke verordenende bevoegdheid, met name in relatie tot artikel 139b Sr en artikel 441b Sr en in het licht van de AVG?	p. 26
8. Kan een verordening inspelen op nieuwe digitale ontwikkelingen ten opzichte van slimme deurbelcamera's, zoals het verbieden van specifieke nieuwe features?	p. 28
9. Is het mogelijk dat een gemeentelijke verordening specifieke productvoorschriften oplegt, zoals het gebruik van een afsluitbaar klepje dat moet worden opgetild bij het aanbellen of andere vormen van privacy-by-design?	p. 29
10. Ethische analyse	p. 30
11. Afsluitend	p. 43
12. Disclaimer	p. 44
Bijlage 1	p. 45

1 Inleiding

- 1.1 Steeds vaker vervangen burgers hun traditionele deurbel door een zgn. slimme deurbel.¹ Slimme deurbellen combineren een deurbel met een beveiligingscamera. In Nederland zijn inmiddels ruim 1,2 miljoen slimme deurbellen in gebruik, wat leidt tot toenemende zorgen over privacy en toezicht in de openbare ruimte. Specifieke beroepsgroepen, zoals postbezorgers, worden vaak ongewenst en herhaaldelijk gefilmd. Bovendien worden beelden regelmatig gedeeld via sociale media, met autoriteiten zoals gemeenten en politie, of automatisch geüpload naar de cloud (opslag). Dat brengt (privacy)risico's met zich mee.
- 1.2 De juridische en ethische vraagstukken met betrekking tot het gebruik van slimme deurbelcamera's door particulieren en bedrijven leiden steeds vaker tot rechtszaken² en klachten³ bij de Autoriteit Persoonsgegevens ("AP"). Gemeenten worstelen met de vraag wat er vanuit gemeentelijk perspectief mogelijk, wenselijk en toegestaan is rondom het gebruik van slimme deurbellen. Zij benoemen de verantwoordelijkheid om de grondrechten van hun inwoners en bezoekers te beschermen en sociale cohesie in wijken te waarborgen.
- 1.3 Naar aanleiding hiervan is de Adviesfunctie verantwoord datagebruik ("Adviesfunctie") gevraagd om advies uit te brengen over – kort samengevat – de vraag (i) of er privacyrechtelijke bezwaren bestaan tegen het gebruik van slimme deurbellen die gericht zijn op de openbare weg en (ii) of het mogelijk is om in een algemene plaatselijke verordening ("APV") regels te stellen over het gebruik van slimme deurbellen. De vragen van de VNG zien kortom op de mogelijkheden tot regulering van het gebruik van slimme deurbelcamera's, de reikwijdte van gemeentelijke bevoegdheden in dit verband en de mogelijkheden om via gemeentelijke verordeningen voorwaarden te stellen aan het gebruik slimme deurbelcamera's.

¹ Een slimme deurbelcamera is een elektronische deurbel die is uitgerust met een camera, microfoon en vaak ook een luidspreker, waarmee op afstand via een internetverbinding live videobeelden kunnen worden bekeken en (in veel gevallen) kunnen worden opgenomen. Daarnaast beschikt een slimme deurbel doorgaans over aanvullende functies zoals bewegingsdetectie, notificaties via een app, en soms gezichtsherkenning of integratie met andere slimme apparaten.

² Zie bijvoorbeeld: rb. Overijssel 5 maart 2025, ECLI:NL:RBOVE:2025:1232; rb. Zeeland-West-Brabant 30 september 2024, ECLI:NL:RBZWB:2024:9059; rb. Den Haag 4 september 2024, ECLI:NL:RBDHA:2024:17862; en rb. Overijssel 28 november 2023, ECLI:NL:RBOVE:2023:4831.

³ Zie bijvoorbeeld: <https://autoriteitpersoonsgegevens.nl/actueel/camera-van-de-buren-grote-ergernis-ap-wil-preventieve-aanpak-deurbelcameras>; <https://www.volkskrant.nl/binnenland/slimme-deurbel-leidt-tot-hausse-aan-privacyklachten~b521e5d0/>; <https://www.nu.nl/tech/6302614/slimme-deurbel-leidt-tot-golf-aan-privacyklachten-bij-toezichthouder.html>; <https://www.rtl.nl/nieuws/artikel/5436617/ruim-1000-klachten-een-jaar-over-slimme-deurbel-toezichthouder-maakt-zich>; en <https://www.security.nl/posting/830825/AP+ontvangt+veel+klachten+over+deurbelcamera%27s%3A+groet+deel+hangt+illegaal>.

2 Vraagstelling rapport

2.1 In dit rapport worden de volgende vragen beantwoord:

1. In hoeverre is het op grond van de Algemene Verordening Gegevensbescherming ("**AVG**") voor burgers en bedrijven toegestaan om gebruik te maken van slimme deurbelcamera's die mede zijn gericht op de openbare weg ter bescherming van zichzelf en hun eigendommen?
2. Hoe verhoudt artikel 6, eerste lid, aanhef en onder f, AVG zich tot de grondrechten van passanten, in het bijzonder het recht op privacy dat wordt gewaarborgd door artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden ("**EVRM**")?
3. In hoeverre bestaat er aan de zijde van de gemeente juridische ruimte om het gebruik van slimme deurbelcamera's die een deel van de openbare weg filmen, bij gemeentelijke verordening (APV) te reguleren?
4. Wat is de reikwijdte van de gemeentelijke verordenende bevoegdheid, met name in relatie tot artikel 139b van het Wetboek van Strafrecht ("**Sr**") en artikel 441b Sr en in het licht van de AVG?
5. Kan een gemeentelijke verordening inspelen op nieuwe digitale ontwikkelingen ten opzichte van slimme deurbelcamera's, zoals het verbieden van specifieke nieuwe features?
6. Is het mogelijk dat een gemeentelijke verordening specifieke productvoorschriften oplegt, zoals het gebruik van een afsluitbaar klepje dat moet worden opgetild bij het aanbellen of andere vormen van privacy-by-design?

3 Managementsamenvatting

3.1 In dit rapport komen wij tot de volgende bevindingen:

In hoeverre is het op grond van de AVG voor burgers en bedrijven toegestaan om gebruik te maken van slimme deurbelcamera's die mede zijn gericht op de openbare weg ter bescherming van zichzelf en hun eigendommen?

Op basis van de wet, jurisprudentie, Richtsnoeren⁴ van de EDPB en de Beleidsregels van de AP inzake cameratoezicht, zijn wij van mening dat particulieren en bedrijven – op grond van hun gerechtvaardigd belang ter bescherming van zichzelf en hun eigendommen – met hun slimme deurbelcamera's het onvermijdelijke deel van de openbare weg mogen filmen, mits zij daarbij ook voldoen aan de overige vereisten van de AVG, waaronder die met betrekking tot de verwerking van bijzondere en strafrechtelijke persoonsgegevens (artikelen 9 en 10 AVG), behoorlijkheid en

⁴ Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur en Richtsnoeren 1/2024 inzake de verwerking van persoonsgegevens op grond van op grond van artikel 6, lid 1, onder f, van de AVG.

transparantie, doelbinding, privacy by design en beveiliging.⁵ Met het 'onvermijdelijke deel' doelen wij op het deel van de openbare ruimte voor het filmen waarvan in de context van de inzet van slimme deurbelcamera's in specifieke gevallen een grondslag bestaat als bedoeld in artikel 6, eerste lid, aanhef en onder f, AVG.

Hoe verhoudt artikel 6, eerste lid, aanhef en onder f, AVG zich tot de grondrechten van passanten, in het bijzonder het recht op privacy dat wordt gewaarborgd door artikel 8 EVRM?

Indien de betreffende (rechts)persoon een gerechtvaardigd belang heeft, en daarbij voldoet aan de overige randvoorwaarden van de AVG (zie randnrs. 4.5 t/m 4.22) is daarmee automatisch gegeven dat de inzet van het cameratoezicht ook rechtmatig is op grond van artikel 8 EVRM. Artikel 6, eerste lid, aanhef en onder f, AVG voorziet bij wet in de inbreuk die het cameratoezicht maakt op het recht op de persoonlijke levenssfeer van passanten.⁶

In hoeverre bestaat er aan de zijde van de gemeente juridische ruimte om het gebruik van slimme deurbelcamera's die een deel van de openbare weg filmen, bij gemeentelijke verordening (APV) te reguleren?

Naar ons oordeel is artikel 6, eerste lid, aanhef en onder f, AVG uitputtend beoogd en is het uitgesloten dat de gemeente middels een APV ingrijpt in het gerechtvaardigde belang van de betrokkene om het onvermijdelijke deel van de openbare weg te filmen. Dus op het moment dat er een grondslag onder de AVG bestaat voor de inzet van de slimme deurbelcamera. Voor het vermijdelijke deel van de openbare weg, waarin er in beginsel dus geen grondslag in de AVG is voor de inzet van een slimme deurbelcamera, staat de AVG op zichzelf niet in de weg aan gemeentelijke regulering. Echter ook in dat geval houdt de regulering van onrechtmatige inzet van slimme deurbelcamera's enkel juridisch stand voor zover door de gemeente toereikend gemotiveerd kan worden dat met de regulering een geheel ander doel dan het doel dat de AVG heeft (bescherming van privacy en gegevensbescherming) wordt nagestreefd, bijvoorbeeld de handhaving van de openbare orde. Wij achten het op voorhand op zijn minst twijfelachtig of een dergelijke openbare ordeverstoring per definitie kan worden aangenomen in geval van het filmen van de openbare weg. Ook voor zover de regulering van de onrechtmatige inzet van slimme deurbelcamera's niet kan worden aangemerkt als toezicht op of handhaving van de AVG, is het de vraag of de AVG wel ruimte biedt aan de gemeentelijke wetgever om, ter bescherming van persoonlijke levenssfeer en persoonsgegevens van voorbijgangers, de (reeds verboden en aldus onrechtmatige) verwerking van persoonsgegevens nader te reguleren bij APV. Dat is geen uitgemaakte zaak.⁷

⁵ Zie paragraaf 4.

⁶ Zie paragraaf 5.

⁷ Zie paragraaf 6.

Wat is de reikwijdte van de gemeentelijke verordenende bevoegdheid, met name in relatie tot artikel 139b Sr en artikel 441b Sr en in het licht van de AVG?

Zoals reeds toegelicht in paragraaf 6 is het sterk de vraag of gemeentelijke regulering een aanvulling mag vormen op de AVG. Als die drempel (toch) gehaald wordt, dan zal de gemeentelijke regelgeving óók binnen de grenzen van het Wetboek van Strafrecht (Sr) moeten blijven. In dat kader zal de APV-verbodsbepaling naar zijn aard en motief moeten verschillen van de verbodsbepalingen van artikel 139b en/of artikel 441b Sr. Deze bepalingen strekken sec tot het beschermen van de persoonlijke levenssfeer. Reeds dit verschil in motief maakt dat zich geen wezenlijk risico (meer) voordoet dat met de APV-verbodsbepalingen in strijd wordt gehandeld met de bovengrens van deze artikelen, mits een dergelijke APV-bepaling niet hetzelfde handelen reguleert.⁸

Kan een verordening inspelen op nieuwe digitale ontwikkelingen ten opzichte van slimme deurbelcamera's, zoals het verbieden van specifieke nieuwe features?

Bij het verbieden van specifieke nieuwe features, zien wij dezelfde juridische belemmeringen en risico's als beschreven bij paragraaf 6. Voor de beantwoording van deze vraag verwijzen wij dus naar paragraaf 6.⁹

Is het mogelijk dat een gemeentelijke verordening specifieke productvoorschriften oplegt, zoals het gebruik van een afsluitbaar klepje dat moet worden opgetild bij het aanbellen of andere vormen van privacy-by-design?

Voor de beantwoording van deze vraag verwijzen we naar paragraaf 6. Het maakt voor de ruimte in een gemeentelijke verordening om slimme deurbelcamera's te reguleren niet uit of sprake is van een verbod of (slechts) van beperkingen in de zin van productvoorschriften. Voor de beantwoording van deze vraag verwijzen wij dus naar paragraaf 6.¹⁰

Ethische analyse

In aanvulling op de juridische analyse zijn de ethische risico's van het gebruik van deurbelcamera's geanalyseerd en de mogelijkheden om deze, al dan niet door middel van aanvullende regelgeving, te mitigeren. Tegen de achtergrond van de begrippen 'responsible by design' en 'betekenisvolle, menselijke controle', zijn vijf vragen behandeld:

1. Is het wenselijk om het gebruik van slimme deurbelcamera's aan banden te leggen vanwege ethische informatiebeveiligingsrisico's?
2. Hebben slimme deurbelcamera's onwenselijke ethische consequenties op sociaal vlak?

⁸ Zie paragraaf 7.

⁹ Zie paragraaf 8.

¹⁰ Zie paragraaf 9.

3. Zijn er ethische risico's m.b.t. het respecteren van belangen van passanten en omwonenden?
4. Hoe groot is het risico van 'function creep', waarbij de toepassing verschuift naar surveillance of biometrische categorisering, en is dit een ethische grond voor aanvullende regulering?
5. Zijn er technische aanpassingen van slimme deurbelcamera's mogelijk die de ethische risico's uit de eerdere vragen mitigeren?

De behandeling van de vragen leidt tot de identificatie een vijftal ethische risico's voor de belanghebbenden (eigenaren, overheden, omwonenden en passanten, en leveranciers): misbruik bij gebrekkige informatiebeveiliging; sociale erosie; ondermijning van zelfbeschikking; gebrek aan uitlegbaarheid; en function creep. In het licht van de door de risico's geraakte publieke waarden (rechtvaardigheid, respect, saamhorigheid, transparantie, veiligheid en vrijheid) zijn voor ieder ethisch risico gerichte aanbevelingen gedaan aangaande toezicht, voorlichting van belanghebbenden en mogelijke technische, impact verminderende maatregelen. De voorliggende perspectieven zijn gericht aan gemeenten, maar kunnen ook voor een organisatie zoals de Autoriteit Persoonsgegevens relevant zijn voor het formuleren van handavingsmogelijkheden en het treffen van maatregelen. Omwonenden en passanten blijken de voornaamste risicodragers te zijn, maar er zijn ook risico's voor eigenaren en overheden. Aan de hand van waardenspanningen zijn de ethische relaties tussen belanghebbenden rondom slimme deurbelcamera's geanalyseerd, waarbij voornamelijk spanningen tussen (i) eigenaren van de deurbellen en omwonenden en passanten; en (ii) tussen eigenaren van de deurbellen en overheden aan het licht komen. De ethische risico's voor omwonenden en passanten die betrekking hebben op transparantie, respect en vrijheid komen in aanmerking om m.b.v. technische en informationele maatregelen (gedeeltelijk) gemitigeerd te worden.

Voornamelijk de risico's die gelden voor omwonenden en passanten en hun relatie met de eigenaren van de deurbel vragen om een respons, waarbij het belangrijk is dat lokale overheden waar nodig samenwerken met toezichthouders om maatregelen te treffen en voorlichting vorm te geven. Er wordt daarom geadviseerd om als gemeente of andere aan regulering denkende organisatie niet alleen naar de juridische mogelijkheden te kijken, maar ook naar wat er daarnaast mogelijk is om de overblijvende ethische risico's te mitigeren. De voorliggende ethische analyse vormt daarvoor een startpunt.

4 In hoeverre is het op grond van de AVG voor burgers en bedrijven toegestaan om gebruik te maken van slimme deurbelcamera's die mede zijn gericht op de openbare weg ter bescherming van zichzelf en hun eigendommen?

Materiële reikwijdte AVG

Voordat wordt toegekomen aan een inhoudelijke beantwoording van de vraag in hoeverre het op grond van de AVG voor burgers en bedrijven is toegestaan om gebruik te maken van slimme deurbelcamera's die mede zijn gericht op de openbare weg ter bescherming van zichzelf en hun eigendommen, dient eerst te worden vastgesteld of het gebruik van slimme deurbelcamera's door particulieren überhaupt valt onder de reikwijdte van de AVG. Camerabeelden die door slimme deurbelcamera's worden vastgelegd, bevatten persoonsgegevens. De AVG is alleen van toepassing, voor zover van belang, als de verwerking van persoonsgegevens valt onder de materiële reikwijdte van de AVG. De materiële reikwijdte van de AVG volgt uit artikel 2 AVG:

"1. Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

2. Deze verordening is niet van toepassing op de verwerking van persoonsgegevens:

a) in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen;

b) door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, VEU vallen;

c) door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit;

d) door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. (...)" (onderstreping toegevoegd)

- 4.1 Op grond van artikel 2, tweede lid, aanhef en onder c, AVG valt de verwerking van persoonsgegevens door een natuurlijke persoon in het kader van een zuiver persoonlijke of huishoudelijke activiteit niet onder het toepassingsbereik van de AVG.¹¹ Deze zgn. vrijstelling voor huishoudelijke activiteiten dient in het geval van cameratoezicht restrictief te worden uitgelegd en ziet uitsluitend op verwerkingen die plaatsvinden binnen het persoonlijke of gezinsleven van de verwerkingsverantwoordelijke.¹²

¹¹ Zie ook overweging 18 uit de considerans van de AVG.

¹² HvJEU 11 december 2014, C-212/13, ECLI:EU:C:2014:2428 (*František Ryneš*); en overweging 18 uit de considerans van de AVG.

- 4.2 Wij nemen tot uitgangspunt dat in geval van de inzet van een slimme deurbelcamera die een deel van de openbare weg filmt, geen sprake (meer) is van een verwerking die uitsluitend plaatsvindt voor persoonlijke of huishoudelijke doeleinden. De gebruiker van de slimme deurbelcamera dient in zoverre te voldoen aan de verplichtingen van de AVG. Het is vaste rechtspraak van het Europese Hof van Justitie ("HvJEU") dat een verwerking die zich uitstrekt tot de publieke ruimte niet als louter privé kan worden aangemerkt.¹³ Ook anderszins kan naar onze mening worden betwijfeld of sprake is van 'persoonlijk gebruik', aangezien bij slimme deurbelcamera's doorgaans een externe verwerker betrokken is die vaak op enige wijze de beelden op een externe locatie verwerkt.

Gerechtvaardigd belang (artikel 6, eerste lid, aanhef en onder f, AVG)

- 4.3 In artikel 6, eerste lid, AVG is bepaald dat iedere (rechtmatige) verwerking van persoonsgegevens, waaronder mede begrepen de verstrekking van persoonsgegevens, moet worden gebaseerd op een zgn. verwerkingsgrondslag.

- 4.4 In het kader van cameratoezicht door burgers en bedrijven is met name de verwerkingsgrondslag "gerechtvaardigd belang" (artikel 6, eerste lid, aanhef en onder f, AVG) relevant. Deze bepaling luidt als volgt:

"(...) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de 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."

- 4.5 Uit de Europese en nationale rechtspraak volgt dat een verwerking op grond van artikel 6, eerste lid, aanhef en onder f, AVG slechts rechtmatig is voor zover aan drie cumulatieve voorwaarden is voldaan:

- i) met de verwerking wordt een *gerechtvaardigd belang* van de verwerkingsverantwoordelijke of van een derde nagestreefd;
- ii) de verwerking is *noodzakelijk* (en in overeenstemming met het proportionaliteits- en subsidiariteitsbeginsel); en
- iii) er is een *belangenafweging* verricht tussen de belangen van de verantwoordelijke/de derde enerzijds en de betrokkenen anderzijds en uit de belangenafweging is gebleken dat de fundamentele rechten en vrijheden van betrokkenen niet prevaleren.¹⁴

¹³ HvJEU 11 december 2014, C-212/13, ECLI:EU:C:2014:2428 (*František Ryneš*), punt 33. Dit volgt ook uit nationale rechtspraak, waarin in het kader van burenruzies over deurbelcamera's wordt getoetst aan de AVG. Zie bijvoorbeeld: rb. Zeeland-West-Brabant 10 januari 2023, ECLI:NL:RBZWB:2023:166. Zie ook: ABRvS 26 februari 2020, ECLI:NL:RVS:2020:594.

¹⁴ Zie bijvoorbeeld: HvJEU 29 juli 2019, ECLI:EU:C:2019:629 (*Fashion ID*), HvJEU 4 mei 2017, C-13/16, ECLI:EU:C:2017:336 (*Rigas satiksme*), HvJEU 4 juli 2023, ECLI:EU:C:2023:537 (*Meta vs Bundeskartellamt*), punt 106 e.v., HvJEU 7 december 2023, ECLI:EU:C:2023:958 (*SCHUFA II*), HvJEU 12 september 2024, ECLI:EU:C:2024:738 (*Neunte Immobilien*) punt 49-65, HvJEU 4 oktober 2024,

- 4.6 Deze voorwaarden zijn door de European Data Protection Board ("**EDPB**"), specifiek voor het maken van videobeelden, nader uitgewerkt in haar (i) *Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur* en (ii) *Richtsnoeren 1/2024 inzake de verwerking van persoonsgegevens op grond van op grond van artikel 6, lid 1, onder f, van de AVG*.¹⁵

Ad i) Gerechtvaardigd belang

- 4.7 Er moet sprake zijn van een legitiem, concreet en actueel belang van de verwerkingsverantwoordelijke of een derde. Het belang mag niet strijdig zijn met de wet of de fundamentele beginselen van gegevensbescherming. Het gerechtvaardigd belang moet daarbij reëel zijn en betrekking hebben op een actueel probleem; het mag dus niet gaan om een louter fictief of speculatief probleem. Dreigend gevaar kan echter wel een gerechtvaardigd belang opleveren.

- 4.8 Gerechtvaardigde belangen kunnen, in aantoonbaar gevaarlijke situaties, onder meer betrekking hebben op de bescherming van eigendommen, het voorkomen van inbraken in een buurt met een verhoogd inbraakrisico of het waarborgen van de persoonlijke veiligheid van bewoners of werknemers in bedrijfspanden.¹⁶ Cameratoezicht ter beveiliging van personen en eigendommen kan dus slechts worden gebaseerd op de grondslag gerechtvaardigd belang indien de particulier aantoont dat daarmee een gerechtvaardigd belang gemoeid is.

Ad ii) Noodzakelijkheid

- 4.9 De verwerking van persoonsgegevens – in dit geval het maken en gebruiken van camerabeelden waarop personen te zien zijn – moet (strikt) noodzakelijk zijn voor het realiseren van het gerechtvaardigd belang, zoals het beveiligen van eigendommen. Dit houdt in dat de gegevens die worden verwerkt toereikend en ter zake dienend moeten zijn, en beperkt moeten blijven tot wat noodzakelijk is voor het doel van de verwerking (artikel 5, eerste lid, aanhef en onder c, AVG).
- 4.10 De verwerkingsverantwoordelijke dient in alle gevallen vooraf zorgvuldig te beoordelen of het gebruik van een slimme deurbelcamera die mede is gericht op de openbare ruimte geschikt is om het beoogde doel te bereiken, en of deze inzet toereikend en noodzakelijk is. Daarbij geldt dat het gebruik van een slimme deurbelcamera slechts is toegestaan indien het doel van de verwerking niet redelijkerwijs kan worden bereikt met andere middelen die minder ingrijpend zijn voor de fundamentele rechten en vrijheden van de betrokkenen – in dit geval passanten die worden gefilmd.
- 4.11 Dit betekent tevens dat de verwerkingsverantwoordelijke moet onderzoeken of er alternatieve veiligheidsmaatregelen beschikbaar zijn die minder ingrijpend zijn voor de

ECLI:EU:C:2024:857 (*KNLTB*), ABRvS 27 juli 2022, ECLI:NL:RVS:2022:2173, r.o. 7.1 en Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111, r.o. 14.

¹⁵ EDPB, *Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur*, V2.0, vastgesteld op 29 januari 2020; en EDPB, *Richtsnoeren 1/2024 inzake de verwerking van persoonsgegevens op grond van op grond van artikel 6, lid 1, onder f, AVG*, V1.0, vastgesteld op 8 oktober 2024.

¹⁶ EDPB, *Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur*, V2.0, vastgesteld op 29 januari 2020, p. 11.

persoonlijke levenssfeer, maar die even doeltreffend zijn in het voorkomen van bijvoorbeeld inbraak, diefstal of vandalisme. Te denken valt aan maatregelen zoals het plaatsen van een hek, het aanbrengen/verbeteren van verlichting, het aanbrengen van veiligheidssloten en/of het installeren van inbraakwerende ramen en deuren. De verwerkingsverantwoordelijke dient per geval te beoordelen of dergelijke alternatieven een redelijke en effectieve oplossing vormen. Indien dat het geval is, dient te worden afgezien van het gebruik van slimme deurbelcamera's die mede zijn gericht op de openbare ruimte.

- 4.12 De verwerkingsverantwoordelijke moet dus goed kunnen motiveren dat het beoogde doel niet op een andere, minder ingrijpende, wijze kan worden bereikt, en dat het doel – bij het uitblijven van het gebruik van de slimme deurbelcamera – niet of slechts in sterk verminderde mate op efficiënte wijze kan worden gerealiseerd. Ook dient de reikwijdte van het cameratoezicht en de inbreuk op de privacy van passanten beperkt te worden.

Ad iii) Belangenafweging

- 4.13 Naast het bestaan van een gerechtvaardigd belang en noodzaak voor de inzet van een slimme deurbelcamera vereist artikel 6, eerste lid, aanhef en onder f, AVG dat het gerechtvaardigde belang van de verwerkingsverantwoordelijke (of de derde) – bijvoorbeeld het belang van bescherming van diens eigendommen – zwaarder weegt dan de belangen of de fundamentele rechten en vrijheden van de betrokkene. De verwerkingsverantwoordelijke moet daarom beoordelen: 1) in hoeverre het cameratoezicht gevolgen heeft voor de belangen, grondrechten en vrijheden van personen, 2) of dit leidt tot schending van of negatieve gevolgen voor de rechten van betrokkenen en 3) welk belangen zwaarder wegen. De verwerkingsverantwoordelijke moet de risico's op inbreuken op de rechten en vrijheden van betrokkenen kortom zorgvuldig beoordelen. Doorslaggevend daarbij is de mate waarin de verwerking inbreuk maakt op deze rechten.

- 4.14 De grondrechten en fundamentele vrijheden enerzijds en de gerechtvaardigde belangen van de verwerkingsverantwoordelijke anderzijds moeten derhalve zorgvuldig worden beoordeeld en tegen elkaar afgewogen. Het verrichten van een belangenafweging is verplicht. Deze belangenafweging moet voorafgaand aan de verwerking plaatsvinden en wordt mede bepaald door factoren als de aard en omvang van het toezicht, de context waarin dit plaatsvindt, het aantal betrokkenen van wie camerabeelden worden vastgelegd en de verwachting van betrokkenen om wel of niet gefilmd te worden.¹⁷ Daarbij is onder meer van belang of het cameratoezicht plaatsvindt in een omgeving waarin personen zich vrij moeten kunnen bewegen, zoals de openbare ruimte.¹⁸ De uitleg van het begrip "redelijke verwachtingen" mag niet

¹⁷ Het gebruik van cameratoezicht in bijvoorbeeld een afgelegen gebied moet anders worden beoordeeld dan het gebruik van cameratoezicht in een drukbezocht of stedelijk gebied, aangezien de context en de te verwachten impact op de privacy van betrokkenen wezenlijk verschillen.

¹⁸ Betrokkenen mogen ook verwachten dat zij niet worden gefilmd in openbaar toegankelijke gebieden, met name wanneer die gebieden doorgaans worden gebruikt voor ontspanning en recreatie, of waar mensen gaan zitten en/of elkaar treffen, zoals bankjes, tafels in restaurants, parken, bioscopen en

alleen gebaseerd zijn op de subjectieve verwachtingen van de betrokkene. Het beslissende criterium moet veeleer zijn of een objectieve derde redelijkerwijs mocht verwachten dat hij in die specifieke situatie zou worden gefilmd.¹⁹ Borden die betrokkenen informeren over het cameratoezicht zijn op zichzelf genomen niet bepalend voor de beoordeling van wat een betrokkene objectief redelijkerwijs mag verwachten. Het enkele feit dat een bord aanwezig is, betekent niet dat voorbijgangers automatisch de redelijke verwachting zouden moeten hebben dat zij worden gefilmd.²⁰

- 4.15 Voorts dient te worden beoordeeld of er minder ingrijpende middelen beschikbaar zijn om hetzelfde doel te bereiken.²¹ De mate van ingrijpendheid kan onder meer worden beoordeeld aan de hand van het type informatie dat wordt verzameld (de inhoud), de reikwijdte van de verwerking (zoals informatiedichtheid en ruimtelijk of geografisch bereik), het aantal betrokkenen (zowel in absolute aantallen als relatief ten opzichte van de populatie), de concrete context van de verwerking, de feitelijke belangen van de betrokken groep, de beschikbaarheid van minder ingrijpende alternatieve middelen, en de aard en omvang van de gegevensverwerking.
- 4.16 Uit de rechtspraak en de richtlijnen van de Europese privacy toezichthouders maken wij op dat in de regel vrij snel wordt aangenomen dat aan de zijde van een burger of een bedrijf een belang bestaat om cameratoezicht in te stellen. Dit lijkt naar ons oordeel in gelijke zin te gelden voor de inzet van slimme deurbelcamera's. Wel wordt daarbij kritisch gekeken naar de maatregelen die in het licht van dataminimalisatie en privacy by design zijn getroffen. Het gaat daarbij om het treffen van aanvullende maatregelen om de ongewenste gevolgen van cameratoezicht zoveel mogelijk te beperken, zoals het automatisch wissen van camerabeelden na twee weken, het beveiligen van een videorecorder met een wachtwoord en het bijhouden van logbestanden van toegangspogingen tot een app waarmee de beelden konden worden geraadpleegd.

Zie ABRvS 26 februari 2020, ECLI:NL:RVS:2020:594:

"[belanghebbende A] en [belanghebbende B] hebben de camera's geplaatst om hun eigendommen te beschermen evenals de eigendommen en personen die aan hun zorg zijn toevertrouwd. In geval van een incident kunnen zij met de camerabeelden onderbouwd aangifte doen. Niet in geschil is dat dit op zich een gerechtvaardigd belang is als bedoeld in artikel 6, eerste lid, aanhef en onder f, van de AVG. Dat dit belang daadwerkelijk aanwezig is, blijkt uit het eierincident. Dat van dit incident geen aangifte is gedaan en dat het niet tegen het bedrijf zou zijn gericht, is in dat kader niet van belang.

fitnessvoorzieningen. Hier zullen de belangen of de rechten en vrijheden van de betrokkenen vaak zwaarder wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke. Zie EDPB, Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur, V2.0, vastgesteld op 29 januari 2020, p. 14.

¹⁹ Vgl. overweging 47 uit de considerans van de AVG.

²⁰ Zie EDPB, Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur, V2.0, vastgesteld op 29 januari 2020, p. 14.

²¹ EDPB, Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur, V2.0, vastgesteld op 29 januari 2020, p. 11-12.

Naar aanleiding van het handhavingsverzoek heeft de AP de feitelijke situatie ter plaatse onderzocht. In de stukken bevinden zich prints van stilgezette camerabeelden van 10 april 2018, de dag waarop de AP ter plaatse is geweest. Op deze foto's is te zien dat de perceelgrens met het toegangshek en een stuk van de openbare weg in beeld wordt gebracht. Er bestaat geen aanleiding om niet uit te gaan van de door de AP op die dag vastgestelde situatie ter plaatse. De rechtbank heeft terecht overwogen dat niet meer personen op de weg in beeld worden gebracht dan noodzakelijk is om het doel van het cameratoezicht te bereiken. Ook van buiten het perceel kan schade worden aangericht, waardoor het noodzakelijk is ook een gedeelte buiten de perceelgrens op camera vast te leggen. Alleen personen die zich dichtbij de perceelgrens bevinden, komen volledig in beeld. Als alleen de berm in beeld wordt gebracht, zijn personen niet direct identificeerbaar. De AP mocht, zoals de rechtbank terecht heeft overwogen, het zwaarwegende belang van [belanghebbende A] en [belanghebbende B] om hun eigendommen te beschermen zwaarder laten wegen dan het belang van voorbijgangers op de openbare weg, aangezien zij zo min mogelijk in beeld worden gebracht. Daarnaast hebben [belanghebbende A] en [belanghebbende B] maatregelen getroffen om de ongewenste gevolgen van cameratoezicht zoveel mogelijk te beperken, zoals het wissen van de beelden na twee weken, het beveiligen van de videorecorder met een wachtwoord en het bijhouden van logfiles van inlogpogingen op de app waarmee toegang wordt verschaft tot de beelden. Ook worden voorbijgangers geïnformeerd over het cameratoezicht, zoals hierna onder 5.1 wordt overwogen. Dat de AP naar aanleiding van het onderzoek ter plaatse verdere aanbevelingen heeft gedaan, betekent niet dat sprake was van een overtreding van de AVG. Deze aanbevelingen zijn gegeven om de bescherming van persoonsgegevens verder te optimaliseren. [belanghebbende A] heeft vervolgens per e-mail toegezegd de gedane aanbevelingen uit te voeren.” (onderstreping toegevoegd)

- 4.17 Voor bedrijven geldt dat de noodzaak van videobewaking voor de bescherming van het bedrijfsgebouw en personeel zich beperkt tot de buitengrenzen van het betreffende terrein. De AP neemt als uitgangspunt dat een private organisatie hier slechts toe gerechtigd is voor zover het in beeld brengen van deze delen van de openbare ruimte onvermijdelijk is ter beveiliging van personen en goederen die aan hun zorg zijn toevertrouwd.

Zie Beleidsregels van de AP inzake cameratoezicht (Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens, openbare versie – 28 januari 2016), p. 41:

“Voorbeeld niet onvermijdelijk

Een avondsupermarkt filmt de openbare weg grenzend aan de winkel, omdat daar vaak geluidsoverlast plaatsvindt door uitgaande jongeren. De avondsupermarkt wil deze beelden verstrekken aan de politie en de gemeente zodat zij maatregelen gaan treffen tegen de overlast. De handhaving van de openbare orde is echter voorbehouden aan de gemeente. De avondsupermarkt heeft niet aangetoond dat het cameratoezicht

onvermijdelijk is ter beveiliging van personen en goederen die aan zijn zorg zijn toevertrouwd. Dit cameratoezicht is derhalve ongeoorloofd.

Voorbeeld niet onvermijdelijk

Een supermarkt heeft bij de ingang van de winkel een camera geplaatst tegen winkeldiefstal. De camera filmt de openbare weg. De supermarkt heeft niet aangetoond waarom video-opnames van alleen de winkel, zoals van de schappen en de kassa's, onvoldoende effectief is tegen winkeldiefstal. Er is in dit geval geen sprake van een noodzaak om de openbare weg te filmen, zodat dit cameratoezicht ongeoorloofd is.

Voorbeeld onvermijdelijk

Een juwelier heeft bij de ingang van de winkel een camera geplaatst tegen beroving. De camera filmt een klein gedeelte van de openbare weg dat direct aan de ingang van de winkel grenst. Dit gedeelte van de openbare weg wordt gefilmd, omdat is gebleken dat overvallers zich vlak voor de winkel vermommen voordat ze de winkel betreden. De juwelier heeft aangetoond dat het onvermijdelijk is om een dit kleine gedeelte van de openbare weg te filmen om zijn zaak goed te kunnen beveiligen. Dit cameratoezicht is derhalve geoorloofd."

- 4.18 De EDPB hanteert, in haar Richtsnoeren over de verwerking van persoonsgegevens door middel van videoapparatuur, een vergelijkbaar criterium.²²

"In het algemeen beperkt de noodzaak van videobewaking voor de bescherming van de bedrijfsgebouwen van verwerkingsverantwoordelijken zich tot de buitengrenzen van het betreffende terrein. In bepaalde gevallen is de bewaking van het terrein zelf echter niet voldoende voor een doeltreffende bescherming. In specifieke gevallen kan het noodzakelijk zijn de videobewaking uit te breiden naar de directe omgeving van het terrein. In dit geval moet de verwerkingsverantwoordelijke fysieke en technische maatregelen overwegen, bijvoorbeeld het afschermen of pixeleren van niet-relevante gebieden."

- 4.19 In het verdere vervolg van dit rapport gaan wij ervan uit dat particulieren, op grond van hun gerechtvaardigd belang ter bescherming van zichzelf en hun eigendommen, met hun slimme deurbelcamera's het onvermijdelijke deel van de openbare weg mogen filmen. Met het 'onvermijdelijke deel' doelen wij in de rest van dit advies op het deel van de openbare ruimte voor het filmen waarvan in de context van de inzet van slimme deurbelcamera's in specifieke gevallen een grondslag bestaat als bedoeld in artikel 6, eerste lid, aanhef en onder f, AVG.

Overige juridische randvoorwaarden

- 4.20 Aangezien het in dit rapport met name gaat over de vraag of de inzet van slimme deurbelcamera's kan worden gereguleerd, laten wij de overige juridische randvoorwaarden van de AVG onbesproken. Dit neemt uiteraard niet weg dat particulieren zullen moeten voldoen aan de overige juridische vereisten van de AVG,

²² EDPB, Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur, V2.0, vastgesteld op 29 januari 2020, p. 12.

waaronder die inzake de verwerking van bijzondere en strafrechtelijke persoonsgegevens (artikelen 9 en 10 AVG), behoorlijkheid en transparantie, doelbinding, privacy by design en beveiliging.

5 Hoe verhoudt artikel 6, eerste lid, aanhef en onder f, AVG zich tot de grondrechten van passanten, in het bijzonder het recht op privacy dat wordt gewaarborgd door artikel 8 EVRM?

Indien de betreffende (rechts)persoon een gerechtvaardigd belang heeft, en daarbij voldoet aan de overige randvoorwaarden van de AVG (zie randnrs. 4.5 t/m 4.22) is daarmee automatisch gegeven dat de inzet van het cameratoezicht ook rechtmatig is op grond van artikel 8 EVRM. Artikel 6, eerste lid, aanhef en onder f, AVG voorziet bij wet in de inbreuk die het cameratoezicht maakt op het recht op de persoonlijke levenssfeer van passanten.

- 5.1 De AVG is een uitvloeisel van artikel 8, eerste lid, van het Handvest van de grondrechten van de Europese Unie ("**Handvest**"), waarin is bepaald dat eenieder recht heeft op bescherming van zijn persoonsgegevens.²³
- 5.2 In tegenstelling tot het Handvest maakt het EVRM geen onderdeel uit van het Unierecht. Dit neemt niet weg dat het EVRM wel van belang wordt geacht bij de uitleg van de AVG. Artikel 52, derde lid, van het Handvest bepaalt dat, voor zover het Handvest rechten bevat die overeenkomen met rechten die al zijn gegarandeerd door het EVRM, de inhoud en reikwijdte van die rechten gelijk zijn aan die welke aan het EVRM kunnen worden ontleend. Deze bepaling sluit echter niet uit dat het Unierecht in bepaalde gevallen ruimere bescherming biedt dan het EVRM.
- 5.3 Wij stellen voorop dat artikel 8 EVRM in beginsel regelt dat de overheid zich onthoudt van enige inmenging in het recht op de eerbiediging van privé-, familie- en gezinsleven, waaronder de persoonlijke levenssfeer van de burger. De bescherming artikel 8 EVRM is echter niet absoluut en kan op grond van artikel 8, tweede lid, EVRM worden beperkt.
- 5.4 Artikel 8, tweede lid, EVRM bevat een zgn. beperkingsclausule. Het recht op eerbiediging van het privéleven mag worden beperkt, mits aan de volgende drie cumulatieve voorwaarden is voldaan: de inbreuk moet (i) in overeenstemming met een wettelijke bepaling plaatsvinden; (ii) een legitiem doel nastreven en; (iii) noodzakelijk zijn in een democratische samenleving.

²³ Dit blijkt onder meer uit overweging 1 uit de considerans van de AVG: "De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht. Krachtens artikel 8, lid 1, van het Handvest van de grondrechten van de Europese Unie (het "Handvest") en artikel 16, lid 1, van het Verdrag betreffende de werking van de Europese Unie (VWEU) heeft eenieder recht op bescherming van zijn persoonsgegevens."

- 5.5 In onderhavig rapport staat niet de inmenging van de Staat in de persoonlijke levenssfeer centraal, maar de inmenging van een particulier die inbreuk maakt op de persoonlijke levenssfeer van passanten door (een deel van) de openbare weg te filmen.
- 5.6 In de rechtspraak van het EHRM en de nationale rechtspraak wordt aangenomen dat artikel 8 EVRM ook werking heeft tussen burgers onderling (zogenoemde 'horizontale werking').
- 5.7 Niet in alle gevallen waarin een (slimme deurbel)camera (deels) op de openbare weg is gericht, is sprake van een inbreuk op de persoonlijke levenssfeer in de zin van artikel 8 EVRM.²⁴ Of een handeling een inbreuk vormt, hangt mede af van de vraag of een persoon redelijkerwijs een verwachting van privacy mocht hebben.²⁵ In de publieke ruimte geldt dat personen zich er in redelijkheid van bewust moeten zijn dat zij kunnen worden gezien of herkend en dat hun gedrag kan worden waargenomen door anderen. Verder is van belang in hoeverre de gegevens een bepaalde persoon betreffen, in hoeverre de gegevens worden verwerkt en gebruikt en of ze worden gepubliceerd op een wijze die verder gaat dan wat gewoonlijk voorzienbaar is. Ook de duur van de opslag van de persoonsgegevens is in deze context van belang.²⁶
- 5.8 Indien echter wél sprake is van een inbreuk op de persoonlijke levenssfeer, neemt de rechter, vergelijkbaar met de AVG-rechtspraak, tot uitgangspunt dat artikel 8 EVRM in beginsel niet in de weg staat aan het plaatsen van (slimme deurbel)camera's ter beveiliging van de eigen woning of het bedrijfspand, of ter waarborging van de veiligheid van werknemers, mits dit cameratoezicht strikt noodzakelijk, proportioneel en in overeenstemming met het subsidiariteitsbeginsel is (er zijn geen lichtere middelen voorhanden om hetzelfde doel te bereiken).²⁷ In dat geval dient een belangenafweging plaats te vinden tussen de conflicterende belangen van degene die het cameratoezicht heeft ingesteld en de passanten ten aanzien van wie een inbreuk wordt gemaakt op de persoonlijke levenssfeer.
- 5.9 Wij laten een gedetailleerde bespreking van de relevante rechtspraak met betrekking tot artikel 8 EVRM in relatie tot (particulier) cameratoezicht voor dit rapport achterwege, aangezien een particulier in beginsel ook altijd zal moeten voldoen aan de AVG bij de inzet van een slimme deurbelcamera. Indien de betreffende (rechts)persoon een gerechtvaardigd belang heeft, en daarbij voldoet aan de overige randvoorwaarden van de AVG (zie randnr. 4.5 t/m 4.22), is daarmee automatisch gegeven dat de inzet van het cameratoezicht ook rechtmatig is op grond van artikel 8 EVRM. Artikel 6, eerste lid, aanhef en onder f, AVG voorziet bij wet in de inbreuk die het cameratoezicht maakt op het recht op de persoonlijke levenssfeer van passanten.

²⁴ Zie bijvoorbeeld: EHRM 17 juli 2003, ECLI:CE:ECHR:2003:0717JUD006373700, punt 40; ABRvS 21 februari 2018, ECLI:NL:RVS:2018:590, r.o. 10.2; en Hof Amsterdam 5 februari 2019, ECLI:NL:GHAMS:2019:529, r.o. 9.3.

²⁵ Rb. Rotterdam 24 oktober 2018, ECLI:NL:RBROT:2018:9358, r.o. 4.10 en 4.11. Zie ook: EHRM 22 september 2010, ECLI:CE:ECHR:2010:0902JUD003562305.

²⁶ EHRM 22 september 2010, ECLI:CE:ECHR:2010:0902JUD003562305; en ABRvS 21 februari 2018, ECLI:NL:RVS:2018:590, r.o. 10.2.

²⁷ Zie bijvoorbeeld: rb. Overijssel 25 april 2018, ECLI:NL:ROVE:2018:1513.

6 In hoeverre bestaat er aan de zijde van de gemeente juridische ruimte om het gebruik van slimme deurbelcamera's die een deel van de openbare weg filmen, bij gemeentelijke verordening (APV) te reguleren?

Naar ons oordeel is artikel 6, eerste lid, aanhef en onder f, AVG uitputtend beoogd en is het uitgesloten dat de gemeente middels een APV ingrijpt in het gerechtvaardigde belang van de betrokkene om het onvermijdelijke deel van de openbare weg te filmen. Dus op het moment dat er een grondslag onder de AVG bestaat voor de inzet van de slimme deurbelcamera. Voor het vermijdelijke deel van de openbare weg, waarin er in beginsel dus geen grondslag in de AVG is voor de inzet van een slimme deurbelcamera, staat de AVG op zichzelf niet in de weg aan gemeentelijke regulering. Echter ook in dat geval houdt de regulering van onrechtmatige inzet van slimme deurbelcamera's enkel juridisch stand voor zover door de gemeente toereikend gemotiveerd kan worden dat met de regulering een geheel ander doel dan het doel dat de AVG heeft (bescherming van privacy en gegevensbescherming) wordt nagestreefd, bijvoorbeeld de handhaving van de openbare orde. Wij achten het op voorhand op zijn minst twijfelachtig of een dergelijke openbare ordeverstoring per definitie kan worden aangenomen in geval van het filmen van de openbare weg. Ook voor zover de regulering van de onrechtmatige inzet van slimme deurbelcamera's niet kan worden aangemerkt als toezicht op of handhaving van de AVG, is het de vraag of de AVG wel ruimte biedt aan de gemeentelijke wetgever om, ter bescherming van persoonlijke levenssfeer en persoonsgegevens van voorbijgangers, de (reeds verboden en aldus onrechtmatige) verwerking van persoonsgegevens nader te reguleren bij APV. Dat is geen uitgemaakte zaak. Wij lichten dit hierna toe.

6.1 De regulering van het gebruik van slimme deurbelcamera's door de gemeente wordt begrensd door de zogenoemde *territoriale grens* (of *zijgrens*), *ondergrens* en *bovengrens*. Kort en goed houden deze grenzen het volgende in:

- **Zijgrens:** gemeenten kunnen enkel regels stellen voor zover het een aangelegenheid betreft die zich op eigen grondgebied afspeelt (zijgrens).
- **Ondergrens:** de gemeenteraad mag daarnaast op basis van artikel 149 Gemeentewet ("Gemw") enkel verordeningen maken die hij *in het belang van de gemeente nodig oordeelt*. Dit houdt – simpel gezegd – in dat gemeenten alleen onderwerpen in een verordening mogen regelen die in voldoende mate aan het publieke belang raken en dus niet alleen een inmenging vormen in de private belangen van hun inwoners. Daarnaast kunnen onderwerpen die in overwegende mate private belangen raken, toch uitstraling hebben naar de openbare ruimte. Ook die belangen mogen gemeenten zich dan aantrekken. Dit wordt wel *de ondergrens* (of:

benedengrens) genoemd.²⁸

- **Bovengrens:** tot slot mag decentrale regelgeving niet conflicteren met hogere regelgeving (artikel 121 Gemw). Daarbij gaat het met name om landelijke wet- en regelgeving, de Grondwet, EU-recht en internationale verdragen die in hetzelfde onderwerp voorzien. In dat kader zijn de volgende vragen relevant:

Voorvraag: In hoeverre bestaan er reeds bepalingen in hogere regelgeving die het gebruik van slimme deurbelcamera's reguleert?

Vraag 1: In hoeverre is de hogere regelgeving op dat onderwerp uitputtend bedoeld?

Hogere wet- en regelgeving is uitputtend bedoeld als bepalingen uit deze wet- en regelgeving in uitgangspunt alles over het desbetreffende onderwerp beogen te regelen. Als dat het geval is, dan mag de gemeentelijke verordening alleen regels bevatten indien daaraan een ander motief ten grondslag ligt. Als de hogere wet- of regelgeving niet uitputtend bedoeld is, dan mogen gemeenten in beginsel zelf regels stellen, tenzij dit hogere regelgeving doorkruist (zie hierna).

Vraag 2: Doorkruist de gemeentelijke verordening (het doel van) de hogere regelgeving (op onaanvaardbare wijze)?²⁹

- 6.2 Aangezien wij in geval van het reguleren van het gebruik van slimme deurbelcamera's geen wezenlijke juridische belemmeringen zien die voortvloeien uit de zij- of ondergrens³⁰, zullen wij ons in dit rapport beperken tot de vraag of, en zo ja, hoe de beoogde regulering zich verhoudt tot de bovengrens. Hieronder treft u onze analyse aan.

Voorvraag: In hoeverre bestaat er reeds hogere regelgeving die het gebruik van slimme deurbelcamera's reguleert?

- 6.3 Zoals uitgebreid toegelicht in paragraaf 4 van dit rapport, vormt de AVG een relevante vorm van hogere regelgeving die de verwerking van persoonsgegevens, ook door middel van een slimme deurbelcamera, reguleert. Particulieren kunnen aan artikel 6,

²⁸ Zie o.a. de Conclusie van P-G E.J. Hofstee van 2 juni 2020, ECLI:NL:PHR:2020:517, overweging 18 e.v.; ABRvS 17 april 2013, ECLI:NL:RVS:2013:BZ7770, r.o. 3.1; en ABRvS 21 september 2011, ECLI:NL:RVS:2011:BT2130, r.o. 2.4.1.

²⁹ Zie wederom de Conclusie van P-G E.J. Hofstee van 2 juni 2020, ECLI:NL:PHR:2020:517, overweging 29; en verder o.a.: HR 24 september 2021, ECLI:NL:HR:2021:1360, r.o. 3.1.1-3.1.10; en ABRvS 15 mei 2019, ECLI:NL:RVS:2019:1583, r.o. 2.2.

³⁰ Wij denken bij de ondergrens bijvoorbeeld aan het belang van de regulering van de openbare ruimte als zodanig en de bescherming van de digitale rechten van de inwoners van de gemeente. Gemeenten worden nu eenmaal verantwoordelijk gehouden voor wat er in de openbare ruimte gebeurt. Wij gaan er dus in uitgangspunt van uit dat aan de ondergrens voldaan wordt. Dat kan anders worden op het moment dat een gemeente regels stelt over slimme deurbellen die uitsluitend kunnen worden opgevat als een inmenging in de private belangen van hun inwoners en niet (ook) raken aan het publieke belang. De ondergrens blijft dus wel een aandachtspunt.

eerste lid, aanhef en onder f, AVG een gerechtvaardigd belang ontlenen om het onvermijdelijke deel van de openbare weg te filmen, mits aan de eisen uit dit artikel wordt voldaan (zoals dat dit noodzakelijk is voor de bescherming van zichzelf of diens eigendommen) en ook aan de overige voorwaarden uit de AVG wordt voldaan. Voor het filmen van de vermijdelijke delen van de openbare weg zal in de context van de inzet van slimme deurbelcamera's per definitie geen grondslag in de zin van artikel 6 AVG bestaan. Belangrijk voor dit rapport is voorts dat het toezicht op de naleving van de AVG exclusief is toebedeeld aan de AP. Daarmee is bij hogere regelgeving uitgesloten dat de gemeente een deel van deze toezicht- en handhavingstaak van de AP overneemt.

Vraag 1: Is deze hogere wet- en regelgeving "uitputtend" bedoeld?

- 6.4 Nu sprake is van relevante hogere regelgeving, rijst de vraag of de AVG e.e.a. uitputtend regelt. Als dat het geval is, dan mag de gemeentelijke APV alleen regels bevatten indien daaraan een ander motief ten grondslag ligt en deze regulering niet de (doelstelling van de) AVG doorkruist. Als de AVG niet uitputtend is bedoeld, dan mag de gemeenten in uitgangspunt zelf (aanvullende) regels stellen.
- 6.5 De AVG heeft primair tot doel om natuurlijke personen een hoog beschermingsniveau te bieden op het gebied van verwerking van persoonsgegevens.³¹ Het doel van de AVG is om een 'consistent en hoog beschermingsniveau te bieden' en de belemmeringen voor het verkeer van persoonsgegevens, die bestonden door de gefragmenteerde wijze waarop persoonsgegevens werden beschermd, op te heffen. De AVG schrijft in dat verband voor dat de bescherming van persoonsgegevens in alle lidstaten 'gelijkwaardig' dient te zijn. De Uniewetgever neemt tot uitgangspunt dat de AVG zorgt voor 'een in de gehele Unie coherente en homogene toepassing van de regels inzake bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens'.

Zie overweging 9 en 10 van de considerans bij de AVG:

"9. 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

³¹ Zie overweging 1-10 van de considerans bij de AVG.

toe te schrijven aan de verschillen in de uitvoering en toepassing van Richtlijn 95/46/EG.

10. Teneinde natuurlijke personen een consistent en hoog beschermingsniveau te bieden en de belemmeringen voor het verkeer van persoonsgegevens binnen de Unie op te heffen, dient het niveau van bescherming van de rechten en vrijheden van natuurlijke personen op het vlak van verwerking van deze gegevens in alle lidstaten gelijkwaardig te zijn. Er moet gezorgd worden voor een in de gehele Unie coherente en homogene toepassing van de regels inzake bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens. (...)” (onderstreping toegevoegd)

Zie ook overweging 13 van de considerans bij de AVG:

“Teneinde natuurlijke personen in de gehele Unie een consistent niveau van bescherming te bieden en te voorkomen dat verschillen het vrije verkeer van persoonsgegevens op de interne markt hinderen, is een verordening nodig om marktdeelnemers, met inbegrip van kleine, middelgrote en micro-ondernemingen, rechtszekerheid en transparantie te bieden, te voorzien in dezelfde wettelijk afdwingbare rechten voor natuurlijke personen in alle lidstaten en in verplichtingen en verantwoordelijkheden voor de verwerkingsverantwoordelijken en de verwerkers, te zorgen voor consistent toezicht op de verwerking van persoonsgegevens en voor vergelijkbare sancties in alle lidstaten, alsook voor doeltreffende samenwerking tussen de toezichthoudende autoriteiten van verschillende lidstaten. (...)”

6.6 Wij stellen voorop dat de AVG een Europese *verordening* is. Dat houdt in dat de nationale wetgever zeer beperkte ruimte heeft om op het terrein van de verwerking van persoonsgegevens zelf regels te stellen. Het doel van een verordening is juist om de regelgeving in alle EU-landen te harmoniseren. Bij de AVG ligt dat overigens genuanceerd. De Uniewetgever heeft ten aanzien van een aantal aspecten van de AVG de mogelijkheid open gelaten om bij lidstatelijk recht nadere regels te stellen. Het gaat daarbij (onder meer) om het vaststellen van:

- verwerkingsgrondslagen in de zin van artikel 6, eerste lid, aanhef en onder c en e, AVG, oftewel: het in het nationale recht creëren van een wettelijke plicht of publieke taak waarvoor het verwerken van persoonsgegevens noodzakelijk is (zie artikel 6, derde lid, AVG);
- grondslagen die de verdere verwerking van persoonsgegevens toestaat (artikel 6, vierde lid, AVG);
- grondslagen voor de verwerking van strafrechtelijke persoonsgegevens (artikel 10 AVG);
- grondslagen voor geautomatiseerde besluitvorming, waaronder profilering (artikel 22, tweede lid, sub b, AVG); en
- wettelijke beperkingen op de AVG-rechten (waaronder de informatieplicht) of de beginselen van artikel 5 AVG (artikel 23 AVG).

- 6.7 De wetgever heeft gebruikgemaakt van deze ruimte door op deze punten onder meer in de UAVG nadere regels vast te stellen. Er is dus wel enige ruimte (gelaten) voor de lidstaten om eigen regels op het gebied van de bescherming van persoonsgegevens te stellen. De (Nederlandse) wetgever merkt zelf ook op dat de rol van de nationale wetgever bij de AVG niet is uitgespeeld. De wetgever wijst er onder meer op dat de AVG op diverse terreinen meer als een Europese richtlijn fungeert, waardoor de nationale wetgevers nog ruimte hebben om keuzes te maken.³² Ook in de rechtspraak wordt deze ruimte gezien.

Zie bijvoorbeeld: Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, r.o. 6.29:

“Met de keuze van het rechtsinstrument van de Verordening heeft de Europese wetgever het belang onderstreept dat op Europees niveau wordt gehecht aan een zorgvuldige omgang met (persoons)gegevens. De AVG regelt de bescherming van gegevens in Nederland aldus in beginsel uitputtend. Tegelijkertijd laat de AVG op onderdelen ruimte voor de nationale wetgeving. Voor zover dat het geval is, geldt de UAVG.”

- 6.8 De vraag rijst aldus of ten aanzien van artikel 6, eerste lid, aanhef en onder f, AVG enige juridische ruimte bestaat om wettelijke beperkingen op te werpen. Dergelijke ruimte lijkt, voor wat betreft het door particulieren filmen van het onvermijdelijke deel van de weg – mits daarvoor een grondslag in de zin van artikel 6 AVG bestaat³³ –, in zijn geheel afwezig. De AVG sluit immers iedere wettelijke beperking van het gerechtvaardigde belang van particulieren uit. Het HvJ EU neemt tot uitgangspunt dat artikel 6, eerste lid, AVG een uitputtende en limitatieve lijst bevat van de gevallen waarin de verwerking van persoonsgegevens als rechtmatig kan worden aangemerkt.³⁴ Het is, mede gezien het voorgaande, vaste rechtspraak van het HvJ EU dat het lidstaten niet vrijstaat om een beroep op het gerechtvaardigd belang voor bepaalde categorieën verwerkingen op voorhand of categorisch uit te sluiten. Er geldt een zogenoemde negatieve toets; een verwerkingsverantwoordelijke mag ieder gerechtvaardigd belang nastreven, tenzij dat in strijd is met de wet.

Zie in dit verband HvJ 24 november 2011, C-468/10 en C-469/10, ECLI:EU:C:2011:777 (*ASNEF en FECEMD*), punt 48³⁵:

“Behoudens artikel 8 van richtlijn 95/46, dat betrekking heeft op de verwerking van bijzondere categorieën gegevens – welke bepaling in het hoofdgeding niet aan de orde is – verzet artikel 7, sub f, van die richtlijn zich er derhalve tegen dat een lidstaat voor bepaalde categorieën persoonsgegevens categorisch en generiek de mogelijkheid van verwerking uitsluit, zonder ruimte te bieden voor een afweging van de betrokken tegengestelde rechten en belangen in een concreet geval.”

³² *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 9.

³³ Als gezegd nemen wij in dit advies tot uitgangspunt dat dat zo is. vgl. randnr. 4.20 hiervoor.

³⁴ Zie HvJ EU 4 juli 2023, C-252/21, EU:C:2023:537 (*Meta Platforms e.a.*), punt 90.

³⁵ In dit arrest ging het over artikel 7, sub f, van de Richtlijn 95/46 (de Privacy-richtlijn), de voorloper van artikel 6, eerste lid, aanhef en onder f, AVG):

Zie in gelijke zin:

HvJ EU 19 oktober 2016, ECLI:EU:C:2016:779 (*Breyer*), punt. 61-62; en
HvJ EU 11 december 2019, ECLI:EU:C:2019:1064 (*M5A-ScaraA*), punt 53.

Zie ook ABRvS 27 juni 2022, ECLI:NL:RVS:2022:2173 (*Voetbal TV*), r.o. 4:

“Verder heeft de rechtbank geoordeeld dat de toetsing van de AP in dit geval uitgaat van een verkeerde interpretatie van het begrip 'gerechtvaardigd belang' en daarom in strijd is met artikel 6, eerste lid, aanhef en onder f, van de AVG. In de rechtspraak van het Hof van Justitie van de Europese Unie wordt geen duidelijke omschrijving gegeven wat een gerechtvaardigd belang precies is en de interpretatie van de AP dat het - kort gezegd - zou moeten gaan om een rechtsbelang, is in die jurisprudentie dan ook niet als zodanig terug te vinden. Deze uitleg strookt ook niet met de opinie van de Werkgroep artikel 29 (WP29, de voorloper van de European Data Protection Board) uit 2014, en met de visie van Advocaat-Generaal M. Bobek, die in zijn conclusie bij het arrest inzake *Fashion ID* van 29 juli 2019, nr. C-40/17, ECLI:EU:C:2019:629, stelt dat dit een open flexibel begrip is. Bovendien volgt uit de rechtspraak van het Hof van Justitie van de Europese Unie dat het lidstaten niet vrijstaat om een beroep op het gerechtvaardigd belang voor bepaalde categorieën verwerkingen op voorhand of categorisch uit te sluiten.”

- 6.9 Uit het bovenstaande concluderen wij dat de gemeente bij gemeentelijke verordening in ieder geval géén wettelijke beperkingen kan stellen aan de inzet van slimme deurbelcamera's in de situatie dat een particulier een *rechtmatig* gerechtvaardigd belang heeft bij het gebruik van de slimme deurbelcamera, oftewel: voor zover het cameratoezicht zich daarbij beperkt tot het onvermijdelijke deel van de openbare weg en ook wordt voldaan aan alle juridische randvoorwaarden van de AVG.
- 6.10 Voor zover de gemeente aldus bij gemeentelijke verordening wettelijke beperkingen zou willen stellen aan het gebruik van slimme deurbelcamera's, kunnen dergelijke gemeentelijke regels hooguit zien op het filmen van delen van de openbare weg waarvoor de particulier géén wettelijke grondslag in de zin van artikel 6 AVG heeft en welke verwerking van persoonsgegevens dan ook onrechtmatig zal zijn. Uitgaande van de hierboven aangehaalde rechtspraak en de opinies van de EDPB en de AP als beschreven in randnrs. 4.19 t/m 4.20 van dit rapport, gaat het hier aldus om de onrechtmatige inzet van een slimme deurbelcamera, waarbij de slimme deurbelcamera beelden maakt van delen van de openbare weg die niet onvermijdelijk zijn.
- 6.11 Daarbij benadrukken wij dat ook in het geval dat een gemeentelijke verordening zich beperkt tot de regulering van het onrechtmatig filmen van de *vermijdelijke* delen van de openbare weg door particulieren met slimme deurbelcamera, wij juridische discussies voorzien met betrekking tot de bovengrens. Wij wijzen op de volgende risicovolle factoren.
- 6.12 Allereerst kan ook voor de vermijdelijke delen de vraag worden gesteld of de AVG wel ruimte biedt aan de gemeentelijke wetgever om, ter bescherming van persoonlijke

levenssfeer en persoonsgegevens van voorbijgangers, de (reeds verboden en aldus onrechtmatige) verwerking van persoonsgegevens nader te reguleren bij APV. Dat is zeker geen uitgemaakte zaak, omdat dat zou betekenen dat gemeenten iets reguleren dat volgens de AVG verboden is.

- 6.13 Daarbij komt dat de beoogde gemeentelijke verbodsbepaling en de daaraan gekoppelde handhaving in ieder geval niet mag neerkomen op een vorm van toezicht op en handhaving van de naleving van de AVG, waaronder artikel 6, eerste lid, aanhef en onder f, AVG. Het toezicht op de naleving van de AVG, waaronder de inzet van cameratoezicht door particulieren, is immers expliciet toebedeeld aan AP (artikel 51, eerste lid, AVG jo. artikel 6, tweede lid, UAVG).

Zie ook *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 23:

“De verordening biedt de mogelijkheid om één of meerdere toezichthoudende autoriteiten op te richten. In Nederland is het toezicht op de gegevensbescherming belegd bij de Autoriteit persoonsgegevens. Nederland kent geen sectorspecifieke toezichthouders. Er is geen reden om hierin bij de uitvoering van de verordening verandering aan te brengen. Hierom wordt in het onderhavige wetsvoorstel de Autoriteit persoonsgegevens aangewezen als enige toezichthoudende autoriteit in de zin van de Verordening, in artikel 6, tweede lid, van de Uitvoeringswet. Van de gelegenheid van deze implementatiewet is gebruikgemaakt om ook in de wet de naamswijziging van College bescherming persoonsgegevens naar Autoriteit persoonsgegevens in het maatschappelijk verkeer door te voeren. In de Uitvoeringswet wordt hierom consequent gesproken van Autoriteit persoonsgegevens.

De Autoriteit persoonsgegevens is verantwoordelijk voor het toezicht op de naleving van de verordening, teneinde de grondrechten en fundamentele vrijheden van personen te beschermen en het vrije verkeer van persoonsgegevens binnen de Unie te vergemakkelijken. De Autoriteit persoonsgegevens is ook als enige, en daarmee leidende, toezichthouder verantwoordelijk voor de uitvoering van de samenwerking tussen toezichthoudende autoriteiten en voor de toetsing van de conformiteit van de toetsingskaders van verschillende autoriteiten (hoofdstuk VII van de verordening). De voorzitter van de Autoriteit persoonsgegevens is ook namens de nationale toezichthoudende autoriteit lid van het Europees Comité voor gegevensbescherming.” (onderstreping toegevoegd)

- 6.14 In het geval de gemeentelijke regulering van de inzet van slimme deurbelcamera's enkel strekt tot de handhaving van de AVG en de bescherming van privacy in de buitenruimte, zijn wij van oordeel dat daarmee per definitie een inbreuk wordt gemaakt op de exclusieve toezicht- en handhavingsbevoegdheid die aan de AP is toebedeeld. Wij zien in zoverre geen (juridische) ruimte voor gemeenten om een deel van de toezichtstaak van de AP op zich te nemen.
- 6.15 Wij onderkennen dat er in de praktijk juridisch enige onzekerheid lijkt te bestaan over de juridische ruimte om cameratoezicht op de vermijdelijke delen van de openbare

weg te reguleren. Opvallend is bijvoorbeeld dat de AP wél de mening lijkt te zijn toegedaan dat de burgemeester enige mogelijkheid heeft om beperkingen en/of nadere eisen te stellen aan het filmen van de openbare weg door particulieren.

Zie de Beleidsregels van de AP inzake cameratoezicht (Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens, openbare versie – 28 januari 2016), p. 40-41:

“De burgemeester is belast met de handhaving van de openbare orde (artikel 172, lid 1, Gemeentewet). Ook indien private organisaties cameratoezicht hebben ingesteld op delen van openbare plaatsen, blijft de burgemeester verantwoordelijk voor de handhaving van de openbare orde op deze plaatsen. Op welke wijze de burgemeester invulling kan geven aan zijn verantwoordelijkheid, is afhankelijk van de situatie. Zo is het mogelijk dat de burgemeester (camera)toezicht instelt op de openbare plaatsen die mede door de private organisaties worden gefilmd. Een ander voorbeeld is dat de burgemeester eisen stelt aan de reikwijdte van het cameratoezicht op de openbare plaatsen door private organisaties of aan de wijze waarop betrokkenen over dit cameratoezicht moeten worden geïnformeerd.

Voorts geldt dat de burgemeester bevoegd is om overtredingen van wettelijke voorschriften die betrekking hebben op de openbare orde, te beletten of te beëindigen (artikel 172, lid 2, Gemeentewet). Zo kan de burgemeester optreden ingeval de bepalingen van een Algemene Plaatselijke Verordening worden overtreden door de inzet van het cameratoezicht door private organisaties.” (onderstreping toegevoegd)

- 6.16 Wij kunnen het hierboven aangehaalde standpunt van de AP, zonder nadere motivering, juridisch niet goed volgen. Wij stellen voorop dat de door de AP aangenomen bevoegdheid, om eisen en regels te stellen door de burgemeester aan het filmen van de openbare buitenruimte, in ieder geval geen betrekking kan hebben op het filmen van de *onvermijdelijke* delen van de openbare weg door particulieren. Door het beperken van het gerechtvaardigde belang om de onvermijdelijke delen van de openbare weg te filmen ter bescherming van personen en eigendommen, zou immers in strijd worden gehandeld met het verbod om categoriaal het gerechtvaardigde belang van particulieren te beperken (zie randnr. 6.9).
- 6.17 Voor het *vermijdelijke* deel van de openbare weg ligt dit wellicht genuanceerder. Het gerechtvaardigde belang van een particulier strekt zich niet uit tot het filmen van de vermijdelijke delen van de openbare weg. Ten aanzien van de regulering van dergelijke onrechtmatige inzet van slimme deurbelcamera's doet zich in ieder geval niet het juridische probleem voor dat een categoriale inbreuk wordt gemaakt op het gerechtvaardigde belang.

Ander motief?

- 6.18 Het bovenstaande zou genuanceerder kunnen liggen indien gemeenten bij toepassing van hun verordenende bevoegdheid een geheel ander motief (doelstelling) nastreven

dan de doelstellingen die de AVG nastreeft (privacy- en gegevensbescherming). Daarbij zou gedacht kunnen worden aan de doelstelling van de bescherming van de openbare orde. Wij betwijfelen echter op voorhand sterk of de gemeente toereikend kan motiveren dat het onrechtmatig filmen van de openbare weg *per definitie* een inbreuk maakt op de openbare orde binnen de gemeente. Daarvoor is noodzakelijk dat de gemeente onderbouwt dat het filmen van de openbare weg leidt tot een 'concrete of dreigende verstoring van de openbare orde' of tot 'een strafbaar feit dat invloed heeft op de orde en rust in de gemeentelijke samenleving'³⁶. Slechts dan zou immers gesteld kunnen worden dat het optreden tegen het filmen kwalificeert als de handhaving van de openbare orde dat van oudsher wordt gedefinieerd als (i) de daadwerkelijke voorkoming en beëindiging van zich concreet voordoende of dreigende verstoringen van de openbare orde enerzijds en (ii) de algemene, bestuurlijke voorkoming van strafbare feiten die invloed hebben op de orde en rust in de gemeentelijke samenleving anderzijds. Dat lijkt ons in algemene zin lastig te onderbouwen. Bovendien blijft ook bij toepassing van een geheel ander motief staan dat de gemeentelijke verordening niet (het doel van) de hogere regelgeving (op onaanvaardbare wijze) mag doorkruisen (zie hierna).

*Vraag 2: Doorkruist de gemeentelijke verordening (het doel van) de hogere regelgeving (op onaanvaardbare wijze)*³⁷

- 6.19 Aangezien wij de kans groot achten dat de AVG uitputtend is bedoeld, en wij in het beschermen van de openbare orde geen overtuigend motief zien, wordt vooralsnog niet toegekomen aan de beantwoording van deze vraag. Het staat echter vast dat voor zover de regulering sec tot doel heeft om de naleving van de AVG te borgen en de privacy en gegevens van passanten te beschermen, het beoogde verbod en de handhaving daarvan waarschijnlijk in strijd komt met de AVG en het daaruit voortvloeiende exclusieve toezicht van de AP.
- 6.20 Zou de gemeente slagen in haar onderbouwing dat met de regulering van de onrechtmatige inzet van slimme deurbellen een openbaar ordebelang is gemoeid, dan verwachten wij dat bij gemeentelijke regulering van het onvermijdelijke deel sprake is van een doorkruising van (het doel van) de AVG. Bij het vermijdelijke deel is dat wellicht minder evident, al zal ook in dat geval het risico bestaan dat sprake is van een doorkruising van de AVG. Daarnaast dient, los van de AVG, te worden geborgd dat de APV-bepaling niet de verbodsbepalingen van het wetboek van Sr doorkruist die zien op het heimelijk opnemen van personen in de openbare ruimte. Ook dat kan een relevante bovengrens vormen. Zie beantwoording van vraag 7 hierna.

³⁶ *Kamerstukken II 2012/13*, 33 582, nr. 3, p. 4.

³⁷ Zie wederom de Conclusie van P-G E.J. Hofstee van 2 juni 2020, ECLI:NL:PHR:2020:517, overweging 29; en verder o.a.: HR 24 september 2021, ECLI:NL:HR:2021:1360, r.o. 3.1.1-3.1.10; ABRvS 15 mei 2019, ECLI:NL:RVS:2019:1583, r.o. 2.2.

7 Wat is de reikwijdte van de gemeentelijke verordenende bevoegdheid, met name in relatie tot artikel 139b Sr en artikel 441b Sr en in het licht van de AVG?

Zoals reeds toegelicht in paragraaf 6 is het sterk de vraag of gemeentelijke regulering een aanvulling mag vormen op de AVG. Als die drempel (toch) gehaald wordt, dan zal de gemeentelijke regelgeving óók binnen de grenzen van het Wetboek van Strafrecht (Sr) moeten blijven. In dat kader zal de APV-verbodsbepaling naar zijn aard en motief moeten verschillen van de verbodsbepalingen van artikel 139b en/of artikel 441b Sr. Deze bepalingen strekken sec tot het beschermen van de persoonlijke levenssfeer. Reeds dit verschil in motief maakt dat zich geen wezenlijk risico (meer) voordoet dat met de APV-verbodsbepalingen in strijd wordt gehandeld met de bovengrens van deze artikelen, mits een dergelijke APV-bepaling niet hetzelfde handelen reguleert. Wij lichten dit toe.

- 7.1 Het wetboek van Sr kent diverse bepalingen die zien op het verbieden van het opnemen van beelden of gesprekken die plaatsvinden op de openbare weg. Relevant in dit verband zijn onder meer artikel 139b Sr (het heimelijk opnemen van gesprekken buiten een woning, besloten lokaal of erf met een technisch hulpmiddel) en artikel 441b Sr (het heimelijk vervaardigen van afbeelding van personen op een voor het publiek toegankelijke plaats). Mocht gemeentelijke regulering een aanvulling op de AVG vormen, dan dient zoals gezegd nog te worden getoetst of het betreffende APV-verbod qua bovengrens niet in strijd komt met bestaande strafbaarstellingen in Sr.
- 7.2 Wij stellen in dit verband voorop dat de strafbepalingen van Sr uitdrukkelijk niet zien op het rechtmatig gebruik van camera's, waaronder slimme deurbelcamera's, en aldus überhaupt niet ingrijpen in het gerechtvaardigde belang van particulieren om het onvermijdelijke deel van de weg te filmen. Daar komt voorts bij dat de APV-verbodsbepaling geen kopie/dubbeling mag inhouden van een bestaande verbodsbepaling van het wetboek van Sr. In de APV dient dus een andere gedraging strafbaar te worden gesteld, met een ander motief.

Zie de conclusie van AG Spronken van 2 november 2021,
ECLI:NL:PHR:2021:1028:

"8.3 Op zichzelf is de gemeentelijke regelgever vrij om het onderwerp van een hogere regeling aan te vullen, maar de gemeentelijke regeling mag niet met de hogere in strijd zijn. Aanvullen betekent ook dat de lagere regelgeving geen hogere regelgeving mag kopiëren. De gemeentelijke verordening moet dus een andere gedraging strafbaar stellen dan de hogere regeling, waarbij die gedraging wel aan de door de hogere regeling verboden gedraging mag raken. (...)

8.4 Voor de toepasselijkheid van art. 121 Gemeentewet en de beantwoording van de vraag of een gemeentelijke verordening een hogere regeling mag aanvullen, is het ook van belang of de verordening een onderwerp regelt waarin reeds door een hogere regeling is voorzien. Er is sprake van eenzelfde onderwerp, indien het object van de hogere en de lagere regeling en het

motief of doel ervan hetzelfde zijn. Als het motief van de gemeentelijke verordening afwijkt van het motief van de hogere regeling, wordt aangenomen dat zij een ander onderwerp regelen en kunnen zij, in beginsel, naast elkaar bestaan. Dat motief kan blijken uit de tekst van de regeling, de rubricering van bepalingen (de kopjes in de verordening), de titel van het hoofdstuk in de verordening waarin de betreffende bepaling is opgenomen of uit bijvoorbeeld de considerans.”

7.3 Voor de beantwoording van de vraag van de VNG is aldus bepalend wat de reikwijdte en het motief is van de verbodsbepalingen in het wetboek van Sr.

7.4 Artikel 139b Sr luidt als volgt:

“1. Met gevangenisstraf van ten hoogste drie maanden of geldboete van de derde categorie wordt gestraft hij die, met het oogmerk een gesprek dat elders dan in een woning, besloten lokaal of erf wordt gevoerd af te luisteren of op te nemen, dat gesprek met een technisch hulpmiddel heimelijk:
1°. anders dan in opdracht van een deelnemer aan dat gesprek afluistert;
2°. zonder deelnemer aan dat gesprek te zijn en anders dan in opdracht van zulk een deelnemer opneemt.
2. Artikel 139a, tweede lid, onder 1° en 3°, is van overeenkomstige toepassing.”

7.5 Dit artikel richt zich tegen het afluisteren en opnemen van een gesprek dat elders dan in een woning, besloten lokaal of erf wordt gevoerd, bijvoorbeeld op de openbare weg of in de auto. De verbodsbepaling strekt tot het beschermen van het privéleven van derden tegen bedreigingen die worden veroorzaakt door het gebruik van moderne afluister- en opname apparatuur.

7.6 Voor strafbaarstelling onder deze bepaling is vereist dat het afluisteren of opnemen heimelijk geschiedt. Of sprake is van heimelijkheid hangt af van de omstandigheden van het geval. In het algemeen zal goede zichtbaarheid van het technisch hulpmiddel, waarvan in geval van een slimme deurbelcamera sprake zal zijn, voor het opheffen van de heimelijkheid voldoende zijn. Daarbij wegen wij mee dat het een feit van algemene bekendheid is dat middels slimme deurbellen beelden en geluiden worden geregistreerd. Deze kenbaarheid wordt nog verder vergroot, als de aanwezigheid van een slimme deurbelcamera kenbaar wordt gemaakt door middel van stickers of waarschuwborden. Van belang daarbij is overigens wel dat duidelijk blijkt uit de stickers of enkel beelden of ook geluid geregistreerd wordt.

7.7 Een ‘gesprek’ heeft in de openbare ruimte een andere definitie dan in private sferen. De wetgever licht toe dat geluidsopnamen van een menigte niet onder de reikwijdte van dit artikel vallen, ook als daarin flarden van gesprekken zijn te onderscheiden.³⁸ Dit maakt dat het opvangen van een gesprek door middel van een slimme deurbelcamera niet zonder meer leidt tot strafbare gedragingen.

³⁸ *Kamerstukken II 1967/68, 9419, nr. 3, p. 7.*

7.8 Artikel 441b Sr luidt:

“Met hechtenis van ten hoogste twee maanden of geldboete van de derde categorie wordt gestraft hij die, gebruik makende van een daartoe aangebracht technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, van een persoon, aanwezig op een voor het publiek toegankelijke plaats, wederrechtelijk een afbeelding vervaardigt.”

7.9 Wanneer het cameratoezicht zonder duidelijke aanduiding plaatsvindt ten aanzien van een voor het publiek toegankelijke ruimte³⁹, levert dit een overtreding⁴⁰ van artikel 441b Sr op. Ook deze verbodsbepaling strekt tot de bescherming van de persoonlijke levenssfeer. Voor deze verbodsbepaling geldt dat een live weergave van een persoon, door middel van een aangebrachte of geïnstalleerde camera, een strafbare gedraging oplevert.⁴¹ Ook deze verbodsbepaling strekt tot het beschermen van het privéleven van derden tegen bedreigingen die worden veroorzaakt door het gebruik van moderne af luister- en opname apparatuur.

7.10 Als het handhaven van de openbare orde als motief aan gemeentelijke regulering ten grondslag ligt, dan zal de APV-verbodsbepaling naar zijn aard en motief verschillen van de verbodsbepalingen van artikel 139b en/of artikel 441b Sr. Deze bepalingen strekken immers sec tot het beschermen van de persoonlijke levenssfeer. Daarmee zou het risico op strijd met de bovengrens van bovengenoemde bepalingen afnemen. Tegelijkertijd zal een gemeente die slimme deurbellen via de APV reguleert, goed moeten kunnen onderbouwen wat hun voorschrift toevoegt ten opzichte van deze strafrechtelijke verbodsbepalingen. Of een gemeente hierin slaagt, zal afhankelijk zijn van de insteek en feitelijke onderbouwing die zij geeft in het kader van de openbare orde.

8 Kan een verordening inspelen op nieuwe digitale ontwikkelingen ten opzichte van slimme deurbelcamera's, zoals het verbieden van specifieke nieuwe features?

Bij het verbieden van specifieke nieuwe features, zien wij dezelfde juridische belemmeringen en risico's als beschreven bij paragraaf 6. Voor de beantwoording van deze vraag verwijzen wij dus naar paragraaf 6.

³⁹ Een plaats is voor het publiek toegankelijk wanneer deze feitelijk voor een in beginsel onbeperkt aantal personen toegankelijk is, zoals de openbare weg. Daarnaast is een plaats voor het publiek toegankelijk wanneer deze weliswaar voor een bepaalde groep van personen openstaat, maar die groep in beginsel een onbeperkt aantal personen kan omvatten. Zie *Kamerstukken II* 2000/01, 27 732, 3, p. 5.

⁴⁰ Wij merken op dat artt. 139a-139d Sr misdrijven zijn.

⁴¹ *Kamerstukken II* 2000/01, 27 732, 3, p. 7.

9 Is het mogelijk dat een gemeentelijke verordening specifieke productvoorschriften oplegt, zoals het gebruik van een afsluitbaar klepje dat moet worden opgetild bij het aanbellen of andere vormen van privacy-by-design?

- 9.1 Voor de beantwoording van deze vraag verwijzen we naar paragraaf 6. Het maakt voor de ruimte in een gemeentelijke verordening om slimme deurbelcamera's te reguleren niet uit of sprake is van een verbod of (slechts) van beperkingen in de zin van productvoorschriften. Voor de beantwoording van deze vraag verwijzen wij dus naar paragraaf 6.

10 Ethische analyse

10.1 Inleiding

In aanvulling op de juridische analyse hiervoor zijn tevens de ethische risico's van het gebruik van deurbelcamera's geanalyseerd en de mogelijkheden om deze, al dan niet door middel van aanvullende regelgeving, te mitigeren. Dit hoofdstuk start met een toelichting op het hiervoor gehanteerde kader. Vervolgens wordt aan de hand van een vijftal deelvragen de ethische impact van het gebruik van deurbelcamera's in kaart gebracht. In de paragraaf 10.3 vatten we de bevindingen uit de analyse samen en formuleren we een aantal conclusies en aanbevelingen.

De in deze analyse overwogen ethische risico's zijn geïdentificeerd o.b.v. een ethische voorstudie (opgenomen in *Bijlage 1*). Een 'ethisch risico' in het kader van technologiegebruik is een nadelig effect voor belanghebbenden dat mogelijk kan optreden als gevolg van het gebruik van de technologie.⁴² Aanvullend op dit begrip, maken we gebruik van een theoretisch kader dat behulpzaam is voor het begrijpen van de waardenspanningen rondom het gebruik van slimme deurbellen. In dit theoretisch kader figureren twee begrippen:

- *Responsible by design*: Bij de beoordeling van het gebruik van deurbelcamera's wordt de gedachte van *responsible by design* als uitgangspunt genomen. Dit houdt in dat *voordat* technologie wordt ingezet, er over ethiek, sociale impact en de relatie met de relevante wet- en regelgeving nagedacht moet worden.⁴³ Door bij het ontwerp van digitale technologie over deze zaken na te denken, kunnen sommige ethische, sociale en juridische problemen voorkomen worden. Zonder het toepassen van *responsible by design* loopt men het risico dat die problemen zich (onverwachts) later in de levenscyclus van de technologie laten zien.
- *Betekenisvolle, menselijke controle*. Ten tweede speelt bij sommige ethische risico's de vraag hoe we *betekenisvolle, menselijke controle* kunnen uitoefenen over de slimme deurbellen.⁴⁴ De verschillende partijen die met het systeem interacteren, dienen via hun eigen 'interface' met het systeem een begrijpelijke mate van controle uit te kunnen oefenen. In de interactie met digitale technologie accentueert 'betekenisvolle, menselijke controle' het belang van de waarden respect, transparantie en zelfbeschikking. Telkens achten wij de volgende vraag ook relevant: *wie* moet hier de controle uitoefenen om *welke belanghebbende* te beschermen? En bovendien: welke grenzen kunnen er door burgers zelf effectief gesteld worden?

Beide begrippen ondersteunen (i) de identificatie van ethische risico's en (ii) het formuleren van aanbevelingen t.a.v. de ethische risico's.

10.1.1 De wenselijkheidsvragen

Op basis hiervan zijn de vragen die in de ethische analyse worden behandeld:

1. Is het wenselijk om het gebruik van slimme deurbelcamera's aan banden te leggen vanwege ethische informatiebeveiligingsrisico's?

⁴² D.M. Douglas, J. Lacey, J., en D. Howard, "Ethical risk for AI." *AI and Ethics* 5 (2024): 2189–2203. <https://doi.org/10.1007/s43681-024-00549-9>

⁴³ Zie hiervoor: <https://highberg.com/nl/insights/whitepaper-responsible-by-design-in-de-publieke-sector>.

⁴⁴ S. Umbrello, "Meaningful Human Control over Smart Home Systems: A Value Sensitive Design Approach," *HUMANA.MENTE Journal of Philosophical Studies* 13, no.37 (2020): 40–65. <https://iris.unito.it/retrieve/e27ce430-106c-2581-e053-d805fe0acbaa/315-Article%20Text-1017-1-10-20200716%20%282%29.pdf>.

2. Hebben slimme deurbelcamera's onwenselijke ethische consequenties op sociaal vlak?
3. Zijn er ethische risico's m.b.t. het respecteren van belangen van passanten en omwonenden?
4. Hoe groot is het risico van '*function creep*',⁴⁵ waarbij de toepassing verschuift naar surveillance of biometrische categorisering, en is dit een ethische grond voor aanvullende regulering?
5. Zijn er technische aanpassingen van slimme deurbelcamera's mogelijk die de ethische risico's uit de eerdere vragen mitigeren?

Bij de beantwoording van deze vragen wordt met name gekeken naar ethische redenen die geen betrekking hebben op de handhaving van privacy en gegevensbescherming in het kader van de AVG. Hoewel alle vragen een relatie hebben met het idee *responsible by design*, ziet vraag (3) specifiek op het idee van betekenisvolle, menselijke controle.

De in dit hoofdstuk gepresenteerde inzichten in ethische risico's zijn primair gericht aan de Nederlandse gemeenten, maar zijn meervoudig bruikbaar. Behalve voor gemeenten kunnen aanbevelingen tevens waardevol zijn voor andere organisaties die regulering of maatregelen t.a.v. slimme deurbelcamera's overwegen, zoals de AP.

10.2 **Ethische analyse van wenselijkheidsvragen binnen het juridische kader**

Uit het *Nationaal onderzoek percepties slimme deurbellen* van Slimme Deurbellen Consortium en Ipsos komt naar voren dat respondenten voornamelijk slimme deurbellen hebben omdat ze 'het fijn vinden om op afstand te kunnen zien wie er voor de deur staat' en 'het een veiliger gevoel geeft' (respectievelijk 70% en 62% van de respondenten).⁴⁶ Tegenover de hoofdredenen die er voor consumenten zijn om slimme deurbelcamera's te gebruiken, plaatsen we in deze analyse een aantal ethische risico's. Dit is niet alleen relevant voor de VNG, maar ook voor bezitters van slimme deurbelcamera's en andere burgers. Te meer omdat uit hetzelfde onderzoek blijkt dat deze groepen nog weinig hebben nagedacht over de bijeffecten van slimme deurbelcamera's.

Uit de juridische analyse bleek dat de wetgeving die op het gebruik van de slimme deurbelcamera's van toepassing is de gemeenten weinig ruimte geeft. Kort samengevat is de ruimte van de gemeente beperkt tot handhaven van het filmen van het vermijdelijke deel van de openbare weg, vanuit een ander motief dan handhaving van de AVG (bijvoorbeeld in het kader van de openbare orde). Los van deze bevoegdheidsvraag, kunnen er ook andere, meer ethische redenen zijn die het wenselijk maken om het gebruik van slimme deurbelcamera's aan banden te willen leggen. Deze redenen staan dan los van wat de camera precies waarneemt en hebben met name betrekking op de maatschappelijke effecten van het gebruik van slimme deurbelcamera's, en laten zich niet reduceren tot louter privacy.

Hierna worden vragen t.a.v. de volgende maatschappelijke waarden behandeld:

- Rechtvaardigheid;
- Respect;
- Saamhorigheid;

⁴⁵ Bij '*function creep*' verschuift de oorspronkelijke toepassing naar een andere toepassing, waarvoor weer andere (ethische) risico's gelden. Nadere toelichting volgt in paragraaf 2.4.

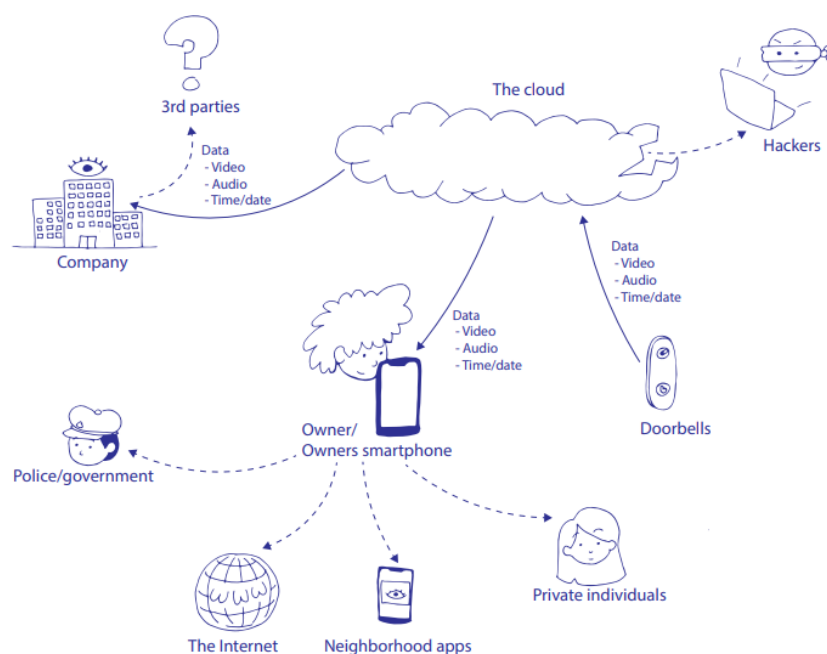
⁴⁶ Slimme Deurbellen Consortium en Ipsos i&o, *Nationaal onderzoek percepties slimme deurbellen*, (juli 2025). <https://privacyfirst.nl/wp-content/uploads/Rapport-onderzoek-Slimme-Deurbellen-Ipsos-IO.pdf>.

- Transparantie;
- Veiligheid; en
- Vrijheid.

Deze publieke waarden komen tevens terug in de samenvattende matrix in par. 10.3.

Verschillende partijen hebben wisselend belang bij het beschermen van bovenstaande waarden. In deze analyse beperken we ons tot de effecten ervan op de volgende groepen:

- Eigenaren van de slimme deurbelcamera's;
- Overheden, zoals gemeenten, politie en justitie
- Leveranciers en ontwerpers van slimme deurbelcamera's;
- Omwonenden;
- Passanten in de openbare ruimte.



Afbeelding 1: Belanghebbendenkaart van de slimme deurbelcamera uit (Torp Dideriksen, 2022)

Iedere volgende paragraaf (10.2.1 t/m 10.2.5) behandelt een van de hoofdvragen gerelateerd aan een ethisch risico. De ethische analyse is t.b.v. de overzichtelijkheid op hoofdlijnen weergegeven. Voor een verdieping verwijzen wij naar *Bijlage 1*, de ethische voorstudie naar de ethische risico's van slimme deurbelcamera's. Deze studie is breder opgezet dan hier in de rapportage is weergegeven, namelijk zonder relatie met het juridische kader.⁴⁷ Per vraag wordt het volgende besproken:

- Het ethische risico onderliggend aan de vraag;
- Voor wie het een risico is en waarom;
- Welke aanbevelingen voor het mitigeren van dit risico relevant zijn.

⁴⁷ De bronnen die geraadpleegd zijn om de ethische analyse te motiveren (juli 2025), zijn gedeeltelijk terug te vinden in de ethische voorstudie. Tijdens de beantwoording van de hoofdvragen (september 2025) is hierop voortgebouwd, maar men heeft niet geschroomd aanvullende relevante informatie en bronnen toe te voegen wanneer dat relevant bleek.

10.2.1 *Is het wenselijk is om het gebruik van slimme deurbelcamera's aan banden te leggen vanwege ethische informatiebeveiligingsrisico's?*

Informatiebeveiliging is een compliance domein op zichzelf. Gebrekkige informatiebeveiliging is echter tevens een bron van ethisch risico, voornamelijk voor degene wiens data of directe omgeving het betreft. Hier bespreken we het ethische risico dat optreedt als een kwaadwillende actor gebruik wil maken van de beelden van de deurbelcamera. Dit is relevant om na te gaan of er bij slimme deurbelcamera's extra aandacht aan dit risico moet worden besteed.

ETHISCH RISICO. (*Misbruik van deurbelcamera bij gebrekkige informatiebeveiliging*) Exploitatie van kwetsbaarheden in de informatiebeveiliging door een kwaadwillende actor.

OMSCHRIJVING. In de afgelopen periode zijn slimme deurbelcamera's meerdere keren in opspraak gekomen vanwege problemen met informatiebeveiliging.⁴⁸ Een voorbeeld uit 2020 laat zien hoe een kwade actor misbruik kan maken van de positionering van de deurbel: de eigenaren van de camera zijn na een hackactie bedreigd en racistisch bejegend.⁴⁹ Een voorbeeld uit 2022 is de kwetsbaarheid van de Ring-deurbel op het gebied van WiFi deauthenticatie.⁵⁰ WiFi deauthenticatie is een hackingaanval waarbij een geauthentiseerde gebruiker wordt losgekoppeld en een kwade actor diens plaats inneemt. Hypothetisch beschouwd kunnen ook passanten hiervan het doelwit zijn. Ook is er vaker sprake geweest van het delen van opnames van deurbelcamera's met daarop gevoelige beelden, al dan niet middels hacking ontvreemd.⁵¹ De veiligheid van de deurbelmodellen die op dit moment worden (en zijn) verkocht vormt daarom een ethisch risico. Mogelijk leidt dit tevens tot een misdrijf of bedreiging van de openbare orde.⁵² Een voorbeeld van een voor de overheid relevant ethisch informatiebeveiligingsrisico is buitenlandse spionage door het hacken van deurbellen van (top)ambtenaren. Het risico op buitenlandse spionage is reëel, omdat er in toenemende mate sprake is van cyberdreigingen. Het op (grote) schaal aanwenden van de beelden van deurbelcamera's zou voor een kwade actor waardevolle informatie kunnen opleveren. Ook is een gerichte cyberaanval op deurbellen van ambtenaren niet vergezocht; er is immers eerder misbruik gemaakt van persoonsgegevens van ambtenaren. Voorbeeld hiervan is het uitvoeren van hackingaanvallen op toegangspassen.

RISICODRAGER. Bij gebrekkige informatiebeveiliging is het voornamelijk de bezitter van de deurbelcamera c.q. de gebruiker van de beelden die risico loopt. Dit omdat het zijn of haar data zijn die gestolen kunnen worden en deze persoon dus het doelwit zou kunnen zijn van mogelijke vervolgacties van de kant van de partij die over de beelden kan beschikken. Degenen die vastgelegd worden op de beelden worden niet als grote risicodragers gezien (los van het privacyrisico dat voor hen speelt). Dit omdat het misbruik dat kwaadwillende actoren zouden kunnen maken van deze beelden zich beperkt tot situaties waarin opnames voor deze personen belastend zijn, wat alleen in uitzonderingssituaties het geval zal zijn. Naast bezitters van deurbellen zijn, zoals

⁴⁸ David Buil-Gil, Steven Kemp, Stefanie Kuenzel, Lynne Coventry, Sameh Zakhary, Daniel Tilley en James Nicholson, "The digital harms of smart home devices: A systematic literature review," *Computers in Human Behavior* 145 (2023): 107770. <https://doi.org/10.1016/j.chb.2023.107770>.

⁴⁹ Buil-Gil, et al., "The digital harms of smart home devices: A systematic literature review."

⁵⁰ Mozilla, "Mozilla Publishes Ring Doorbell Vulnerability Following Amazon's Apathy," 6 juni 2023). <https://www.mozillafoundation.org/en/blog/mozilla-publishes-ring-doorbell-vulnerability-following-amazons-apaty/>.

⁵¹ S. A. Snijder, "How smart is your doorbell?" *MSc Thesis* (Technische Universiteit Delft, 2024). <https://resolver.tudelft.nl/uuid:2005fccc-ddc6-4d2d-b05a-c068233752b3>.

⁵² Het op grote schaal hacken van opnames deurbelcamera's kan tevens een risico zijn m.b.t. Nederlands digitale autonomie. Omdat hier tot op heden hier nog weinig onderzoek naar is gedaan, laten we dit in deze analyse buiten beschouwing.

hierboven beschreven, ook de Nederlandse overheid en haar vertegenwoordigers risicodragers.

AANBEVELING. Er zijn geen aanwijzingen dat slimme deurbelcamera's informatiebeveiligingsrisico's introduceren die nieuw zijn voor andere *smart home systems*.⁵³ Hoewel waakzaamheid gepast is, is er geen reden voor regulering die specifiek gericht is op securityrisico's m.b.t. de deurbelcamera's.⁵⁴ Het onderwerp ligt niet in de rede voor gemeentelijke regulering. De toelaatbare kwaliteit van de informatiebeveiliging is een onderwerp voor Nederlandse en Europese warenautoriteiten, niet een onderwerp voor gemeentelijke regulering. Los van die negatieve conclusie, is de positieve conclusie dat er meer bewustzijn gewekt mag worden over het kwaadwillende gebruik van slimme deurbelcamera's dat voortkomt uit gebrekkige informatiebeveiliging. Het is verstandig om de kwaliteit van de informatiebeveiliging van slimme deurbelcamera's te monitoren en als overheid burgers over basismaatregelen te informeren.

VERDIEPING. Zie punt (3) in *Bijlage 1*. Zie voor 'digitale autonomie' punt (4).

- 10.2.2 *Hebben slimme deurbelcamera's onwenselijke ethische consequenties op sociaal vlak?* Het gebruik van slimme cameradeurbellen staat niet los van de bredere ontwikkeling van de maatschappelijke sentimenten omtrent veiligheid. Zoals de focusgroepen van het onderzoek van Slimme Deurbellen Consortium en Ipsos duidelijk maken, is er sprake van een toenemende mate van gevoelens van onveiligheid en argwaan onder Nederlandse burgers over de veiligheid van hun woonomgeving, wat een van de hoofdredenen voor het gebruiken van een slimme cameradeurbel is.⁵⁵ Het gebruik van een slimme cameradeurbel lijkt op het eerste oogpunt een oplossing voor de toenemende angst aangaande de buurt, maar kan ook leiden tot sociale spanningen. Hier gaat het volgende ethische risico over.

ETHISCH RISICO. (*Sociale erosie*) Sociale erosie veroorzaakt door bijeffecten van de 'blik van de deurbel'.

OMSCHRIJVING. Er kan sprake zijn van het ethische risico van sociale erosie doordat men voor de veiligheid overmatig gaat vertrouwen op de deurbelcamera's, in plaats van op het wederzijdse toezicht van burens en sociale controle. Het selectieve beeld van de deurbel en de veiligheid van een 'blik op de weg' kunnen een averechts effect hebben. De perceptie van een afname van veiligheid heeft als effect dat men elkaar in toenemende mate wantrouwt en daardoor surveilleert, wat als bijeffect de vermindering van de sterkte van de lokale sociale cohesie heeft.⁵⁶ Het kan bijdragen aan de onterechte aanname dat mensen in de directe omgeving niet te vertrouwen zijn. Ook kunnen de deurbelcamera's de indruk wekken dat 'gevaarlijke vreemdelingen' zomaar kunnen opduiken. Dit werkt volgens sommigen een 'verklingsamenleving'⁵⁷ in de hand, waarbij geïsoleerde buurtgenoten angstvallig vreemde voorvallen in hun buurt documenteren, interpreteren en delen. Dit kan tevens schadelijke effecten hebben op de mentale gezondheid van burgers, zo vermoedt men. Het effect van sociale erosie kan

⁵³ Arnar Pétursson, "Ethical Hacking of a Ring Doorbell," *MSc Thesis in Computer Science* (KTH Royal Institute of Technology, 2023). <https://www.diva-portal.org/smash/get/diva2:1751192/FULLTEXT01.pdf>.

⁵⁴ Zie *Bijlage 1* voor een aantal technische basismaatregelen voor leveranciers en gebruikers.

⁵⁵ Slimme Deurbellen Consortium en Ipsos i&o, *Nationaal onderzoek percepties slimme deurbellen*, p. 28.

⁵⁶ Thijs Turèl, "Smart doorbell cameras pose a danger to our society," AMS Institute (16 januari 2024). <https://www.ams-institute.org/news/smart-doorbell-cameras-pose-a-danger-to-our-society/>. Zie voor een Nederlandse vertaling: Thijs Turèl, "Slimme deurbellen zijn een gevaar voor onze samenleving," *Trouw* (16 januari 2024). <https://www.trouw.nl/opinie/slimme-deurbellen-zijn-een-gevaar-voor-onze-samenleving~b0d84768/>.

⁵⁷ Privacy First, "De Verklingsamenleving," (16 maart 2024), laatst bijgewerkt op 2 april 2025. <https://privacyfirst.nl/artikelen/de-verklingsamenleving/>.

daardoor geworteld zijn in (i) het idee dat er sprake is van massasurveillance; (ii) het idee veelvuldig geobserveerd te worden door omwonenden; of (iii) confirmatiebias aan de kant van de observerende eigenaar van de cameradeurbel. In de communicatie tussen burgers over slimme deurbelcamera's spelen spanningen over vertrouwen, harmonie, veiligheid, autonomie en vrijheid een rol.⁵⁸

RISICODRAGER. Dit ethische risico wordt gedragen door burgers, namelijk wanneer hun onderlinge sociale banden verslechteren of er vormen van angst door worden versterkt.

AANBEVELING. Bij dit ethische risico is het twijfelachtig of aanvullende regulering een effectieve strategie is om het risico te mitigeren. Als aanbeveling kan worden gedacht aan het informeren van burgers over de mogelijke effecten van slimme deurbelcamera's voor hun buurt. Een (landelijke) informatiecampaagne of buurtbijeenkomsten en -besprekingen zijn middelen die hiervoor gebruikt kunnen worden. Denk hierbij aan een advies om burens en omwonenden in te lichten over het gebruik van een deurbel en waarom daarvoor gekozen, of het maken van afspraken in de buurt over de richting van de cameraleens en hoe lang opnames worden bewaard. Het onderzoek van het Slimme Deurbellen Consortium komt tot een soortgelijke conclusie onder de noemer van 'Kennis verhogen'. Tevens kan gedacht worden aan het introduceren van maatregelen die sociale cohesie moeten vergroten, losstaand van slimme deurbelcamera's om het negatieve effect op de sociale cohesie te compenseren.

VERDIEPING. Zie punt (5) in *Bijlage 1*. Zie ook de bespreking van het begrip 'sousveillance' in punt (2).

10.2.3 *Zijn er ethische risico's m.b.t. het respecteren van passanten en omwonenden?*

Naast privacy zoals bedoeld in de AVG, zijn er andere redenen om aan te denken als het aankomt op het respectvol behandelen van burgers. Hier behandelen we 'zelfbeschikking' en 'uitlegbaarheid'.

ETHISCH RISICO 1. (Ondermijning van zelfbeschikking) De zelfbeschikking van passanten en omwonenden wordt ondermijnd door het gebrek aan 'opt-out' of 'opt-in' mogelijkheden voor interactie met de blik van de slimme cameradeurbel.

OMSCHRIJVING 1. Voor de vastlegging van (bezoekende) passanten is geen sprake van *geïnformeerde toestemming*. Noch is er sprake van een 'opt-in' mogelijkheid, waarbij de bezoeker of passant kiest wat er van haar wordt vastgelegd. De bezoeker of passant is overgeleverd aan de blik van de slimme deurbel, wat tegen diens wil kan zijn. Personen kunnen hierdoor een zogeheten '*chilling effect*' ervaren: het vervreemdende gevoel tot object van observatie gemaakt te worden, dat er tevens toe kan leiden dat men zich anders gaat gedragen dan zonder de aanwezigheid van een camera het geval zou zijn. Het ethische risico is hier dat er sprake is van een gebrek aan betekenisvolle menselijke controle aan de kant van de bezoeker of passant. Los van de relatie met privacy die dit begrip heeft, kan het uitoefenen van een registratieve actie zonder toestemming van betrokkene als niet respectvol worden beschouwd, omdat het inbreuk maakt op hun recht op zelfbeschikking. Dit is een ethisch risico dat zich momenteel op grootschalige basis manifesteert.⁵⁹

ETHISCH RISICO 2. (Gebrek aan uitlegbaarheid) Er wordt niet aan de geobserveerde persoon uitgelegd wat de slimme cameradeurbel doet.

⁵⁸ Snijder, "How smart is your doorbell?".

⁵⁹ Zeming Chen, "A study of ethical issues in developing smart-home technologies," *Medium* (28 april 2021). <https://zc003.medium.com/a-study-of-ethical-issues-in-developing-smart-home-health-technologies-2ff9f7369fea>.

OMSCHRIJVING 2. Het is niet duidelijk voor de geobserveerde persoon (i) hoe hij of zij in beeld komt; (ii) wat er van hem of haar wordt geregistreerd en bewaard; (iii) wie nog meer toegang heeft tot de beelden. Het ethische risico is hier dat er sprake is van een gebrek aan uitlegbaarheid voor de geobserveerde persoon. Dit kan een onveilig gevoel opleveren en ervoor zorgen dat de persoon een interactie met de deurbel heeft die hij of zij niet had willen hebben in het geval hij of zij beter geïnformeerd was.

RISICODRAGER 1 & 2. De risicodrager is in beide gevallen de burger in de rol van omwonende, passant of bezoeker van het huis met een slimme cameradeurbel. Het is namelijk zo dat de zelfbeschikking van deze persoon wordt genegeerd en dat diezelfde persoon niet volledig op de hoogte is wat de slimme cameradeurbel doet (of het aan staat, wat het vastlegt, etc.).

AANBEVELING 1 & 2. Deze ethische risico's hebben gedeeltelijk te maken met het *responsible design* van de slimme deurbelcamera's zelf. Zonder aanpassingen aan de deurbellen kan hier moeilijk iets aan gedaan worden. Anderzijds is het verhogen van transparantie over wat gefilmd wordt en wat er met de beelden gebeurt een passend antwoord op het probleem van 'uitlegbaarheid'. Hierbij kan worden opgemerkt dat maatregelen die enerzijds vanuit privacy-oogpunt van belang zijn, tevens vanuit ethisch perspectief relevant zijn en dus tevens vanuit een ethisch risico gemotiveerd kunnen worden. Voorbeelden hiervan zijn het bieden van opt-out of opt-in mogelijkheden⁶⁰ voor een geobserveerde persoon en het verschaffen van informatie over wat wordt opgenomen en hoe lang beelden bewaard worden. Aanbeveling voor het beperken van het ethische risico m.b.t. uitlegbaarheid is op het niveau van regulering van productvoorschriften van slimme deurbelcamera's expliciet aandacht te hebben voor eisen op het gebied van geïnformeerde toestemming en uitlegbaarheid. Zie par. 10.2.5 voor een bespreking van (soms ad hoc) technische maatregelen die kunnen bijdragen aan het mitigeren van deze ethische risico's.

VERDIEPING 1 & 2. Zie punt (6) in *Bijlage 1*.

10.2.4 *Hoe groot is het risico van 'function creep' en is dit een ethische grond voor aanvullende regulering?*

ETHISCH RISICO. (*Function creep*) De toepassing van slimme deurbelcamera's verschuift naar een ander doel dan waarvoor de technologie bedoeld is.

OMSCHRIJVING. *Function creep* is "een geleidelijke verschuiving van het doel van de technologie, zoals een verschuiving in de richting van meer opdringerigheid of controle."⁶¹ De inzet van de deurbel is gebaseerd op de *toepassing die ontwikkelaars voor ogen hebben*, maar de oorspronkelijke bedoeling van de technologie laat mogelijkheden open voor het 'mogelijke kwaad van de toekomst', oftewel een schadelijke toepassing die mogelijk wordt gemaakt d.m.v. het huidige ontwerp.⁶² Nota bene dat het ontwerp van de deurbel bruikbaar kan zijn voor toepassingen die zowel ten goede als ten kwade kunnen uitpakken. Voorbeeld van *function creep* bij een slimme cameradeurbel zou kunnen zijn het aanwenden van de camerafunctionaliteit voor *biometrische categorisatie* of *surveillance op grote schaal*. Biometrische categorisatie,

⁶⁰ Onder 'opt-out' verstaan we de beginsituatie waarbij de opname aan staat, maar de mogelijkheid om de opname te stoppen aanwezig is. Onder 'opt-in' verstaan we de beginsituatie waarbij de opname uit staat, maar de mogelijkheid om opname te starten aanwezig is.

⁶¹ Centrum voor Ethiek en Gezondheid, *Sensoren in de thuissituatie; de ethiek van e-health deel III*, (2020). <https://www.gezondheidsraad.nl/documenten/adviezen/2020/06/30/sensoren-in-de-thuissituatie>.

⁶² Arne Berger, Albrecht Kurze, Anreas Bischof, Jesse Joshua Benjamin, Richmond Y. Wong en Nick Merrill, "Accidentally Evil: Questionable Values in Smart Home Co-Design," *Conference on Human Factors in Computing Systems (CHI '23)*, April 23– 28, 2023. <https://doi.org/10.1145/3544548.3581504>.

zoals in de verboden categorie van de AI Act bedoeld,⁶³ is mogelijk wanneer de vastgelegde opnamen worden gebruikt om geobserveerde personen in te delen in categorieën die te maken hebben met gevoelige eigenschappen zoals hun sekse, ras, leeftijd, etc. Bij surveillance op grote schaal zouden zowel de cloudaanbieder die de beelden van de deurbel verwerkt, als een overheidsorganisatie die toegang hiertoe kan afdwingen (bijvoorbeeld de politie), deze kunnen gebruiken om een omgeving te monitoren.

In Nederland is door de politie het initiatief 'Camera in Beeld' gestart. Dit behelst het registreren per straat welke beveiligingscamera's beschikbaar zijn, wie de eigenaar is en hoe lang de beelden worden bewaard. Burgers en bedrijven kunnen beveiligingscamera's hiervoor op vrijwillige basis aanmelden.⁶⁴ Beelden die deze camera's maken kunnen dan worden opgevraagd in het geval deze voor onderzoek van waarde kunnen zijn. De politie is niet in staat live mee te kijken,⁶⁵ wat bijvoorbeeld in Los Angeles wel het geval is.⁶⁶ Een ander verschil is dat burgers hun camera's vrijwillig aanmelden, in tegenstelling tot de onvrijwillige overname van de camerabeelden in Los Angeles. Tevens is het privacy- en gegevensbeschermingsrecht van Los Angeles niet gebonden aan de AVG en het EVR. Dit zijn belangrijke, ethische verschillen, omdat in Nederland geen sprake is van actieve surveillance op basis van deze camerabeelden. Privacyorganisatie Bits of Freedom voert echter als bezwaar aan dat de politie door gebruik te maken van beelden van particuliere camera's gebruik maakt van beelden die mogelijk onrechtmatig gemaakt zijn, omdat het filmen van de openbare weg door particulieren in principe niet is toegestaan. Bits of Freedom ziet Camera in Beeld daardoor als buitenwettelijke surveillance-infrastructuur van de politie⁶⁷.

RISICODRAGER. De risicodragers zijn bij de gevallen van *function creep* die hier overwogen worden de burgers, voornamelijk vanuit de rol van passant en omwonende. Echter kunnen er ook alternatieve functies optreden die nadelig zijn voor de eigenaar van de deurbel, zoals surveillance.

AANBEVELING. De risicomitigering die bij *function creep* benodigd is, is sterk afhankelijk van de nieuwe toepassing die mogelijk wordt gemaakt. Ondanks de mogelijkheid dat *function creep* zich voordoet, is het op lokaal niveau reguleren van het gebruik van slimme deurbellen vooralsnog geen verstandige oplossing. Dit is zo omdat, gelijk met wat het geval is voor gebrekkige informatiebeveiliging, de gemeente niet gaat over het toelaten van consumentenproducten op de Nederlandse markt. Echter zijn de voorbeelden van *function creep* geen fictie en vragen ze aldus wel om monitoring en risicomanagement op een landelijk niveau. De ethisch meest risicovolle toepassingen hebben te maken met het toepassen van machine learning (ML) op de opnames van de slimme deurbelcamera's. Een algemene maatregel hierbij is actieve handhaving van de AI Act door de toezichthouders op deze wetgeving. In de voorbeelden die hierboven zijn gegeven – biometrische categorisatie en grootschalige surveillance – zou dit betekenen dat er toezicht dient te zijn op het hergebruik van data door derden (zie hier ook een raakvlak met de AVG). Het primaat voor het voorkomen van *function creep* ligt bij de toezichthouder en niet bij de gemeente. Een goede maatregel zou het regelmatig uitvoeren van producttesten op bestaande en nieuwe modellen deurbelcamera's zijn, om zo kwetsbaarheden en risico's op *function creep* vroegtijdig te onderkennen. Denk

⁶³ Europese Commissie, "AI Act," <https://artificialintelligenceact.eu/ai-act-explorer/>.

⁶⁴ <https://www.politie.nl/informatie/hoe-werkt-camera-in-beeld.html>

⁶⁵ <https://www.politie.nl/informatie/kijkt-de-politie-live-mee-met-mijn-camera.html>.

⁶⁶ D. Calacci, J. J. Shen, en A. Pentland, "The cop in your neighbor's doorbell: Amazon ring and the spread of participatory mass surveillance," *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2 (2022). <https://doi.org/10.1145/3555125>.

⁶⁷ NU.nl, "Videodeurbel pakt inbreker: politie kan beelden van 314.000 camera's opvragen," (18 maart 2023). <https://www.nu.nl/tech-wetenschap/6255431/videodeurbel-pakt-inbreker-politie-kan-beelden-van-314000-cameras-opvragen.html>.

hierbij aan het ethisch hacken van prominente modellen en het openbaar maken van resultaten of het verbieden van de verkoop op specifieke modellen als de resultaten tegenvallen. Vanuit de gedachte *responsible by design* dient gekeken te worden naar de onwenselijke mogelijkheden en hoe alternatieve oplossingen aan burgers geboden kunnen worden. Of dit mogelijk is, verschilt per manifestatie van *function creep*.

VERDIEPING. Zie punt (4) in *Bijlage 1*.

10.2.5 *Zijn er technische aanpassingen van slimme deurbelcamera's mogelijk die de ethische risico's uit de eerdere vragen mitigeren?*

Een van de bevindingen van het onderzoek van het Slimme Deurbellen Consortium en Ipsos is het volgende: "Slimmedeurbelbezitters zijn doorgaans niet geneigd om iets aan te passen aan hun slimme deurbel (zoals het monteren van een privacy schuif, of het veranderen van de instelling van de camera) om privacy-issues mee op te lossen. Niet-slimmedeurbelbezitters [respondentengroep zonder slimme deurbel] vinden de aanpassing in groten getale wel een goed idee, net zoals veel stedelingen en jongeren." Echter is er een aantal technische maatregelen mogelijk dat wel degelijk de hierboven benoemde ethische risico's kan mitigeren.

- **Sticker ter informatie.**

MAATREGEL. Een sticker op de deur of bij de deurbel informeert de bezoeker of passant over de aanwezigheid van de slimme deurbelcamera. Mogelijk kan de sticker ook uitleg geven over de werking van de slimme deurbelcamera. Tevens kan dit bijdragen aan een geïnformeerde toestemming van de kant van de geobserveerde.

EFFECT. Mitigeert de ethische risico's 'gebrek aan uitlegbaarheid' en 'ondermijning van zelfbeschikking'.

- **Beweegbare afscherming van de lens.⁶⁸**

MAATREGEL. Door een afscherming van de lens dient de bezoeker een handeling uit te voeren voordat de camera hem of haar kan filmen. De standaardinstelling is daardoor dat de bezoeker of passant niet wordt gefilmd zolang hij of zij de lens niet vrijmaakt. Dit houdt ook de optie open om uit beeld te blijven.

EFFECT. Mitigeert het ethische risico 'ondermijning van zelfbeschikking'.

- **Visuele cue die aangeeft dat er gefilmd wordt.⁶⁹**

MAATREGEL. Een licht, geluid of beweging van het apparaat maakt aan een passant of bezoeker kenbaar dat hij of zij in beeld komt.

EFFECT. Mitigeert gedeeltelijk het ethische risico 'gebrek aan uitlegbaarheid' omdat er een vorm van communicatie vanuit de deurbel wordt toegevoegd die aan een persoon duidelijk maakt wat de slimme cameradeurbel doet. Echter legt dit niet de werking van deurbel en het datagebruik van de deurbel uit.

- **Anonimisering of blurring.⁷⁰**

MAATREGEL. Gezichten en/of stemgeluid van (bezoekende) passanten worden automatisch wazig gemaakt of anderszins geanonimiseerd.

EFFECT. Mitigeert het ethische risico 'ondermijning van zelfbeschikking'. De relatie met de publieke waarde 'privacy' is dat een anonimiseringsmaatregel voorkomt dat persoonsgegevens worden vastgelegd.

⁶⁸ Bijvoorbeeld: Responsible Sensing Lab, "Shuttering," (z.d.).
<http://responsiblesensinglab.org/nl/projecten/shuttering/>.

⁶⁹ Zie voor voorbeelden: Torp Dideriksen, "Challenging the Concept of Smart Doorbells by Designing New Interactions Based on Privacy"; en Snijder, "How smart is your doorbell?".

⁷⁰ Zie voor voorbeelden Sofie-Amalie Torp Dideriksen, "Challenging the Concept of Smart Doorbells by Designing New Interactions Based on Privacy," *MSc Thesis* (Technische Universiteit Delft, 2022).
challenging_the_concept_of_smart_doorbells_thesis_report.pdf.

- **Process consent.**

MAATREGEL. Het gaat hierbij om het *vernieuwen* van de geïnformeerde toestemming van de persoon om door de deurbel gefilmd te worden.⁷¹ Oftewel, de slimme deurbel verzoekt de bezoeker gedurende de interactie herhaaldelijk om toestemming. De interactie waarin toestemming wordt verleend kan gebaseerd zijn op spraak, waarbij de deurbel letterlijk om actualisering van de toestemming vraagt. Het is ook voorstelbaar dat op het filmen van de deurbel een timer zit, die na een bepaalde periode zorgt dat de deurbel stopt met filmen. In dat geval zou een bezoeker opnieuw op een activatieknop moeten drukken om opnieuw gefilmd te worden.

EFFECT. Mitigeert het ethische risico 'ondermijning van zelfbeschikking'. Heeft ook een relatie met privacy, namelijk dat de bezoeker meer controle uit kan oefenen over de vastlegging van persoonsgegevens dan voorheen.

AANBEVELING. Bovenstaande technische maatregelen zijn aantrekkelijk vanwege hun ethische effecten. Dit betekent echter niet dat lokale regelgeving de toepassing ervan kan voorschrijven. In het kader van het respecteren van omwonenden en passanten en het principe van uitlegbaarheid (dat ook bij AI-systemen een belangrijke rol speelt) zijn er wel productaanpassingen denkbaar die de ethische risico's van 'ondermijning van zelfbeschikking' en 'gebrek aan uitlegbaarheid' mitigeren, zonder daarbij tot handhaving van de AVG te leiden. Kijkende naar de technische opties die in deze paragraaf zijn opgenomen, leiden een 'beweegbare afscherming van de lens' en 'anonymisering of blurring' direct tot privacybescherming. Echter lijkt dat niet het geval te zijn bij de opties 'sticker ter informatie', 'visuele cue die aangeeft dat er gefilmd wordt' of 'process consent', omdat deze opties gericht zijn op het communiceren over de werking van de deurbel en het respecteren van de zelfbeschikking van het geobserveerde individu in het algemeen. Een denkbare maatregel gericht op deze ethische risico's is het kosteloos beschikbaar stellen (bijvoorbeeld door de gemeente) van informatiestickers of zelf te bevestigen beweegbare afschermingen voor de meest gebruikte modellen, begeleid door een (lokale) informatiecampagne. Dit faciliteert het treffen van maatregelen door burgers zelf, zonder dat de gemeente als handhavende partij optreedt. Hierdoor kunnen zo veel mogelijk mensen de voordelen van de slimme deurbelcamera's ervaren, terwijl tegelijkertijd ethische risico's zoveel mogelijk beperkt worden. De maatregelen hebben namelijk als gevolg dat (bezoekende) passanten niet langer of in mindere mate de risicodragers zijn van de ethische risico's 'gebrek aan uitlegbaarheid' en 'ondermijning van zelfbeschikking'. Voor de ethische risico's 'sociale erosie' en '*function creep*' spelen deze technische maatregelen een minder grote rol.

10.3

Conclusie

In deze paragraaf vatten we de bevindingen uit dit hoofdstuk samen. We starten met een overzicht van de effecten voor de verschillende groepen belanghebbenden. Vervolgens geven we een overzicht van de hierbij geconstateerde ethische risico's en de waardenspanning die daarbij optreedt. Het laatste onderdeel van deze paragraaf (10.3.2) bevat een aantal afsluitende overwegingen.

⁷¹ Centrum voor Ethiek en Gezondheid, *Sensoren in de thuissituatie; de ethiek van e-health deel III*. Voor de geïnteresseerden: zie ook het concept 'consent printer' uit Torp Dideriksen, "Challenging the Concept of Smart Doorbells by Designing New Interactions Based on Privacy."

10.3.1 Publieke waarden en effecten op belanghebbenden

Onderstaande matrix geeft voor verschillende groepen belanghebbenden de waardenspanningen weer die gerelateerd zijn aan de eerder beschreven ethische risico's. De tabel maakt onderscheid tussen drie soorten impact: positief (+), negatief (-) en neutraal (+/-). Na de tabel wordt per belanghebbende kort het effectenprofiel toegelicht.

Publieke waarden / Belanghebbenden	Rechtvaardigheid	Respect	Saamhorigheid	Transparantie	Veiligheid	Vrijheid
Eigenaren	+/-	+/-	-	+/-	+	+
Overheden	+	+/-	+/-	+/-	+/-	+/-
Leveranciers en ontwerpers	+/-	+/-	+/-	+/-	+/-	+/-
Omwonenden en passanten	-	-	-	-	-	-

Tabel 1: Belanghebbenden- en waardenmatrix

- *Eigenaren*: Eigenaren ervaren een verbetering van 'Veiligheid' vanwege hun toegenomen vermogen de omgeving te kunnen observeren. Ook qua vrijheid wordt een verbetering ervaren, omdat de slimme deurbel interactiemogelijkheden met bezoekers mogelijk maakt waarover eigenaren eerder niet beschikten. Voor eigenaren worden er positieve noch negatieve effecten ervaren m.b.t. 'Rechtvaardigheid', 'Respect' en 'Transparantie'.
- *Overheden*: Uit de belanghebbenden- en waardenmatrix komt naar voren dat overheden zowel positief als negatief worden beïnvloed slimme deurbelcamera's.⁷² Slimme deurbelcamera's kunnen door overheidsorganisaties aangewend worden voor een positief effect op het gebied van 'Rechtvaardigheid' en 'Veiligheid', bijvoorbeeld wanneer beelden gebruikt worden voor verschaffen van informatie over een misdrijf (zoals het geval is in het kader van Camera in Beeld). Daarnaast is er in het kader van informatiebeveiligingsrisico's zoals spionage en hacking sprake van een tweevormige negatieve invloed voor 'Veiligheid': ten eerste voor de binnenlandse veiligheid in het geval van een spionagedreiging of -poging, en ten tweede voor (top)ambtenaren, vertegenwoordigers van de overheid, in het geval van hacking van individuele deurbellen.
- *Leveranciers en ontwerpers*: Leveranciers en ontwerpers ervaren positieve noch negatieve effecten aangaande de in de matrix opgenomen publieke waarden. Dit komt omdat zij de technologie ontwikkelen en leveren, maar vervolgens niet worden blootgesteld aan de interactie met de deurbel en alleen een commerciële relatie hebben met de overige belanghebbenden. Het gebrek aan effecten is niet verbazingwekkend, aangezien uit het voorgaande bleek dat leveranciers en ontwerpers niet door de geïdentificeerde ethische risico's worden geraakt.
- *Omwonenden en passanten*: Voor de belanghebbendengroep 'omwonenden en passanten' zijn negatieve effecten op de gebieden van 'Rechtvaardigheid', 'Respect', 'Saamhorigheid', 'Transparantie', 'Veiligheid' en 'Vrijheid' waarneembaar. Voor 'Rechtvaardigheid' en 'Vrijheid' zijn de effecten te wijten aan de ondermijning van de zelfbeschikking van geobserveerde personen in

⁷² Zoals eerder gesteld is het mogelijk dat overheden risicodragers zijn op het vlak van digitale autonomie. Over dit risico is echter onvoldoende bekend en vraagt om vervolgonderzoek.

interactie met de deurbel. Voor 'Saamhorigheid' ligt de oorzaak bij het *chilling effect* in toenemende mate geobserveerd te worden: in de eigen buurt kan men zich in mindere mate op zijn of haar gemak voelen. 'Veiligheid' wordt ook negatief geraakt door 'de blik van de deurbel', omdat omwonenden, bezoekers en passanten zich onveilig kunnen voelen onder de blik van de deurbel en het mogelijk is dat kwaadwillende actoren de blik van de deurbel misbruiken ten koste van deze groep. Wat 'Respect' en 'Transparantie' betreft, wordt deze groep negatief geraakt omdat er informatie over de werking van de slimme deurbel niet toegankelijk is voor deze groep (gebrek aan uitlegbaarheid) en de geobserveerden onvoldoende worden geïnformeerd om respectvol te kunnen worden benaderd door de deurbel. Een laatste onderdeel van het negatieve effect op 'Rechtvaardigheid' is de spanning met overheden, die middels vordering van de camerabeelden mogelijk toegang hebben tot onrechtmatige observaties van omwonenden en passanten op de openbare weg.

Een aantal observaties zijn waardevol voor de ethische afwegingen over de ethische risico's en effecten op publieke waarden in het licht van deze effecten voor de belanghebbenden. De ethische risico's worden voornamelijk door omwonenden, passanten en soms de eigenaren zelf gedragen. Ten eerste is het duidelijk geworden dat de ethische baten van de eigenaren op de gebieden van 'Veiligheid' en 'Vrijheid' liggen. Deze baten gaan echter ten koste van 'Saamhorigheid' en 'Rechtvaardigheid' in relatie met andere belanghebbenden (omwonenden en passanten). Ten tweede is het zo dat er binnen het waardenprofiel van leveranciers en ontwerpers geen waarden spanning aanwezig is. Wat wel opvallend is, is de asymmetrie tussen enerzijds leveranciers en ontwerpers, die nauwelijks risico dragen, en anderzijds passanten en omwonenden, die negatief geraakt worden bij alle publieke waarden. De leveranciers en ontwerpers kunnen profiteren van de groeiende vraag naar slimme deurbelcamera's zonder drager te zijn van een ethisch risico. Ten derde valt te zien dat overheden zowel ethische risico's lopen, als ethische baten hebben. Deze baten lijken niet direct ten koste te gaan van de ethische lasten van de risicodragers, behalve in het geval van het gebruik van onrechtmatig verkregen camerabeelden; dan is er sprake van een negatief gevolg voor 'Rechtvaardigheid' bij omwonenden en passanten. Ten vierde kan het gesteld worden dat de voornaamste risicodragers degenen blijken te zijn die de meeste negatieve effecten ervaren bij alle publieke waarden, namelijk omwonenden en passanten. Echter blijkt uit het onderzoek van het Slimme Deurbellen Consortium dat voorbeeldgroepen onder de passanten zich hier (nog) niet per se van bewust zijn.⁷³

Tot slot volgt uit de vorige vier observaties dat de ethische baten voor eigenaren en overheid ten koste gaan van bezoekers, omwonenden en passanten. Hier zien we een twee waarden spanningen. De eerste is een botsing tussen de negatieve effecten op 'Rechtvaardigheid', 'Respect', 'Saamhorigheid', 'Transparantie' en percepties van 'Veiligheid' en 'Vrijheid' voor omwonenden en passanten, en de positieve effecten op 'Vrijheid' en 'Veiligheid' voor eigenaren van de slimme deurbelcamera's. De tweede is een botsing tussen de positieve effecten op 'Veiligheid' en 'Rechtvaardigheid' voor overheden en de negatieve effecten op 'Veiligheid' en 'Rechtvaardigheid' voor omwonenden en passanten.

⁷³ Zie Slimme Deurbellen Consortium en Ipsos i&o, *Nationaal onderzoek percepties slimme deurbellen*, p. 6: over het gebrek aan negativiteit in de houding en leereffect na discussie bij respondenten die voor (vrijwilligers)werk aan de deur komen.

10.3.2 *Ethische risico's en concluderende overwegingen*

Voortbouwend op de effecten op publieke waarden, gerelateerd aan de verschillende belanghebbenden, worden in *Tabel 2* de ethische risico's van slimme deurbelcamera's weergegeven. Op basis van wie de risicodragers per risico zijn en de hierbij geraakte publieke waarden, formuleren we een aantal concluderende overwegingen. Deze overwegingen focussen op wat er mogelijk lijkt om de ethische risico's te adresseren.

Ethisch risico	Primaire risicodrager(s)	Geraakte publieke waarde(n)	Aanbevelingen
<i>Misbruik van deurbelcamera bij gebrekkige informatiebeveiliging</i>	Eigenaren; overheden	Veiligheid	-Monitoren van de kwaliteit van informatiebeveiliging; -Informereren van burgers over technische basismaatregelen.
<i>Sociale erosie</i>	Eigenaren; omwonenden	Saamhorigheid	-Kennis bij burgers verhogen over de ethische risico's van slimme deurbelcamera's in de sociale sfeer; -Burgers ondersteunen bij het faciliteren van gesprekken over het gebruik van slimme deurbelcamera's -Het treffen van maatregelen die sociale cohesie bevorderen.
<i>Ondermijning van zelfbeschikking</i>	Omwonenden en passanten	Rechtvaardigheid; Vrijheid	-Het introduceren van technische of procesmatige verbeteringen van de deurbel, gericht op het faciliteren van een interactie tussen deurbel en geobserveerde.
<i>Gebrek aan uitlegbaarheid</i>	Omwonenden en passanten	Respect; Transparantie	-Het introduceren van technische of procesmatige verbeteringen van de deurbel, gericht op het informeren van de geobserveerde over de werking van de deurbel.
<i>Function creep</i>	Overheden; eigenaren; omwonenden en passanten	Transparantie; Vrijheid, Rechtvaardigheid	-Toezicht op slimme deurbelcamera's op productniveau. -Voorlichting over het gebruik van slimme deurbelcamera's.

Tabel 2: Samenvatting van de bestudeerde ethische risico's

De geïdentificeerde ethische risico's, waardenspanningen en waardenasymmetrie leiden tot aanvullende inzichten over de vraag in hoeverre het mogelijk is het gebruik van slimme cameradeurbellen op gemeentelijk niveau te reguleren en welke aanvullende maatregelen wenselijk zijn. Belangrijk is dat gemeenten zich daar bewust van zijn. Deze ethische risico's laten zich immers slechts ten delen oplossen door juridische maatregelen.

De concluderende aanbeveling is dat gemeenten onderzoeken welke maatregelen aanvullend op het juridisch kader helpen om ethische risico's van het gebruik van deurbelcamera's te beheersen. Nota bene dat de ethische overwegingen ook voor andere organisaties in het overheidsdomein nuttig kunnen blijken. De voorliggende perspectieven zijn gericht aan gemeenten, maar kunnen ook voor een organisatie zoals de AP relevant zijn voor het formuleren van handhavingsmogelijkheden en het treffen van maatregelen. De ethische overwegingen, ethische risico's en inzichten in de impact of belanghebbenden en publieke waarden zijn dus meervoudig bruikbaar.

Als onderbouwing van deze concluderende aanbeveling dienen de aanbevelingen die per ethisch risico zijn gedaan in par. 10.2 hierboven. Deze aanbevelingen zijn niet juridisch van aard, maar kunnen vanuit ethisch perspectief aanknopingspunten zijn voor mogelijke regulering, rekening houdend met de daarbij geldende wettelijke beperkingen, die in de juridische analyse zijn besproken. De verschillende ethische risico's vragen om diverse antwoorden vanuit de overheid en de maatschappij. Echter zijn niet alle risico's geschikt om gemitigeerd te worden middels gemeentelijke regulering en handhaving. Bij het introduceren van aanvullende productvoorschriften gloort wel een mogelijkheid voor regulering die, vanwege de geraakte waarden respect, rechtvaardigheid en transparantie, en de ethische risico's aangaande ondermijning van zelfbeschikking en gebrek aan uitlegbaarheid, het verdient om nog nader onderzocht te worden.

Voornamelijk de risico's die gelden voor omwonenden en passanten en hun relatie met de eigenaren van de deurbel vragen om een respons, waarbij het belangrijk is dat lokale overheden waar nodig samenwerken met toezichthouders om maatregelen te treffen en voorlichting vorm te geven. Om kort te gaan adviseert de adviesfunctie daarom om als gemeente of andere aan regulering denkende organisatie niet alleen naar de juridische mogelijkheden te kijken, maar ook naar wat er daarnaast mogelijk is om de overblijvende ethische risico's te mitigeren.

11 Afsluitend

- 11.1 Tot zover onze analyse. Voor een overzicht van onze conclusies, verwijzen wij u naar de managementsamenvatting in hoofdstuk 3 van dit rapport.

12 Disclaimer

Dit onderzoeksrapport is opgesteld voor en in opdracht van het Ministerie van Binnenlandse Zaken. Anderen dan de opdrachtgever kunnen aan dit onderzoeksrapport geen rechten ontleen. Jegens anders dan de opdrachtgever zijn de opstellers dan ook onder geen enkele omstandigheid aansprakelijk. Niet is uitgesloten dat dit rapport onjuistheden of onvolkomenheden bevat of dat de inhoud van dit rapport inmiddels is achterhaald. Als u advies wenst over een onderwerp dat aan de orde komt in dit rapport, dient u steeds uw eigen (juridische) adviseur te raadplegen.

Op dit rapport zijn de algemene voorwaarden van Pels Rijcken & Droogleever Fortuijn N.V. van toepassing, te raadplegen via <https://www.pelsrijcken.nl/algemene-voorwaarden>.

Bijlage 1

1. Toelichting bij deze bijlage

Highberg heeft een ethisch vooronderzoek verricht ter voorbereiding op het verlenen van een ethisch advies aan de VNG over de adviesvraag welke ethische bezwaren er bestaan ten aanzien van slimme deurbellen die gericht zijn op de openbare weg, t.b.v. het schetsen van de ethische omgeving van de gewenste beperking van het gebruik van slimme deurbelcamera's.

De voorstudie is een bijlage bij het uiteindelijke advies en levert zowel verbreding als verdieping op van het onderwerp. Om een breed beeld te kunnen geven van de ethische risico's en overwegingen t.a.v. slimme deurbelcamera's volgt deze bijlage de volgende structuur:

- §2: *Inleiding van de ethische voorstudie*. De vraagstellingen en de gebruikte ethische begrippen worden geïntroduceerd en toegelicht.

Vervolgens worden in de overige paragrafen specifieke (clusters van) ethische risico's uiteengezet en besproken:

- §3: *Ethische risico's gerelateerd aan informatiebeveiliging*.
- §4: *Function creep, onverantwoord hergebruik voor surveillance en inbreuk op digitale autonomie*.
- §5: *Sociale erosie en mentale gezondheid*.
- §6: *Respect en het doordenken van (sociale groepen) burgers als stakeholders*.

Bij deze ethische voorstudie is een beschouwende bespreking het uitgangspunt. Echter kan en mag niet de illusie van een volledig waardenvrije bespreking gewekt worden. Een aantal morele aannames liggen ten grondslag aan de bespreking die niet zullen worden verdedigd, wat een filosofische exercitie zou worden, maar waarvan wordt aangenomen dat de doelgroep ze deelt. Namelijk: (i) het is onwenselijk als kwaadwillenden gemakkelijk informatiebeveiligingskwetsbaarheid kunnen exploiteren; (ii) niet-proportionele, overmatige surveillance moet vermeden worden; (iii) digitale autonomie is een maatschappelijke waarde die het beschermen waard is; (iv) sociale erosie is onwenselijk, aangezien sterke relaties tussen burgers onderling bijdraagt aan een veerkrachtige democratie; (v) de mentale gezondheid van burgers dient beschermt te worden; (iv) respectvolle interactie met en inclusie van burgers (wanneer relevant) is van belang bij de introductie van nieuwe vormen van overheidshandelen.

2. Inleiding en situering van de vraag

De ethische vragen die betrekking hebben op deurbelcamera's gaan over de wenselijkheid van het gebruik van private camera's gericht de openbare ruimte. We articuleren deze vragen in termen van *ethische risico's*: dit zijn de nadelige effecten voor belanghebbenden die mogelijk kunnen optreden dankzij het gebruik van de technologie.⁷⁴ De ethische risico's vangen verschillende perspectieven, die teruggevoerd kunnen worden op maatschappelijke waarden. Denk hierbij aan (in louter alfabetische volgorde) gezondheid, privacy, rechtvaardigheid, respect, saamhorigheid, solidariteit en veiligheid. Op voorhand kunnen we ook stellen dat er ethische voordelen zijn. Denk bijvoorbeeld de afschrikkende werking die camera's hebben op inbrekers, of, zoals een voorbeeld uit *Trouw* over de diefstal van hondenbrokken illustreert, levert dit type

⁷⁴ D.M. Douglas, J. Lacey, J., en D. Howard, "Ethical risk for AI." *AI and Ethics* 5 (2024): 2189–2203. <https://doi.org/10.1007/s43681-024-00549-9>

deurbellen ook waardevolle informatie op over misdrijven.⁷⁵ De relaties tussen de slimme deurbelcamera's en deze waarden worden in wat volgt nader onderzocht.

Het centrale perspectief dat in de ethische studie wordt aangeboden wordt geïnformeerd door drie begrippen.

- Ten eerste nemen wij bij de beoordeling van het gebruik van deurbelcamera's de gedachte van *responsible by design* als uitgangspunt. Deze gedachte houdt in dat *voordat* technologie wordt ingezet er over ethiek, sociale impact en de relatie met de relevante wet- en regelgeving nagedacht moet worden.⁷⁶ Aan de wieg van het ontwerp is het nuttig dat men deze zaken vertegenwoordigd heeft, zodat zij het uiteindelijke product kunnen informeren en de manifestatie van sommige ethische, sociale en juridische problemen op voorhand voorkomen kan worden. Zonder 'verantwoordelijk te zijn per ontwerp' loopt men het risico dat die problemen zich (onverwachts) later in de levenscyclus van de technologie laten zien.

In wat volgt worden geïdentificeerde ethische risico's gelabeld met '*responsible by design*' om aan te geven dat ze betrekking hebben op een negatief gevolg dat bij het ontwerp van de technologie mogelijk afgevangen had kunnen worden.

- Ten tweede speelt bij sommige ethisch risico's de vraag hoe we *betekenisvolle, menselijke controle* kunnen uitoefenen over de slimme deurbellen.⁷⁷ De verschillende partijen die met het systeem interacteren, dat een onderdeel uitmaakt van een netwerk van andere informatie gedreven systemen, dienen over hun eigen 'interface' met het systeem een begrijpelijke mate van controle uit te kunnen oefenen. Hierbij is het belangrijk respect en zelfbeschikking te bewaken. Telkens achten wij de volgende vraag ook relevant: *wie* moet hier de controle uitoefenen om *welke belanghebbende* te beschermen? En bovendien: welke grenzen kunnen er door burgers zelf effectief gesteld worden?

In wat volgt worden geïdentificeerde ethische risico's gelabeld met '*betekenisvolle, menselijke controle*' om duidelijk te maken dat ze betrekking hebben op de banden aan een slimme cameradeurbel waarvan men zou willen dat ze door een belanghebbende naar wens gelegd kunnen worden.

- Ten derde is er een begrip dat centraal staat in de verandering van de relaties tussen de burger en de overheid, de burger en commerciële partijen en burgers onderling vanwege de introductie van de slimme deurbelcamera: *sousveillance*. Sousveillance is het tegenovergestelde van surveillance, namelijk het 'observeren van onder'. De cameradeurbel is niet de enige sousveillancetechnologie waarover burgers kunnen beschikken. Smartphones en draagbare camera's kunnen ook als observatiemiddelen 'van onderen' aangewend worden. De introductie van monitoringstechnologie bij de voordeur van de burger doet de machtsrelatie met andere partijen veranderen, zowel met externe partijen als met omwonenden en familieleden. De burger wordt in staat

⁷⁵ Eline van Suchtelen, "Slimme deurbel filmt diefstal van hondenbrokken," *Trouw* (12 november 2023). <https://www.trouw.nl/nieuws/slimme-deurbel-filmt-diefstal-van-hondenbrokken~b6ea333e/>.

⁷⁶ Zie hiervoor: <https://highberg.com/nl/insights/whitepaper-responsible-by-design-in-de-publieke-sector>.

⁷⁷ S. Umbrello, "Meaningful Human Control over Smart Home Systems: A Value Sensitive Design Approach," *HUMANA.MENTE Journal of Philosophical Studies* 13, no.37 (2020): 40-65. <https://iris.unito.it/retrieve/e27ce430-106c-2581-e053-d805fe0acbaa/315-Article%20Text-1017-1-10-20200716%20%282%29.pdf>.

gesteld de omgeving te observeren en te dataficeren. Commerciële partijen stellen de burger hiertoe in staat. Zowel burgers als overheden worden het object van deze observaties. Dit doet de bestaande machtsrelaties tussen burgers en overheid en burgers onderling veranderen. Oftewel: de macht om te observeren is niet langer voorbehouden aan bijv. de overheid, maar is nu toegankelijk geworden voor de burger. Dit heeft twee soorten disciplinerende effecten. Het eerste disciplinerende effect is interpersoonlijk en heeft betrekking op burgers onderling. De groeiende aanwezigheid van de blikken van anderen in de openbare ruimte die ze traverseren – los van of de aanwezigheid van deze blikken legaal is – leidt namelijk tot de inhibitie van gedrag aan de kant van de burger.⁷⁸ Dit kan niet alleen plaatsvinden tussen eigenaren van de deurbel, omwonenden, passanten en deur-tot-deurprofessionals zoals pakketbezorgers, maar ook tussen leden van hetzelfde huishouden.⁷⁹ Het tweede disciplinerende effect heeft betrekking op de relatie tussen burger en overheid. Sousveillance kan de vertegenwoordigers van de overheid disciplineren omdat ze vaker geobserveerd en gedocumenteerd worden door burgers, wat een bewustzijn van het eigen handelen afdwingt.⁸⁰

De disciplinerende effecten van sousveillance worden gebruikt in de discussie van de ethische risico's om de totstandkoming en werking van deze risico's te kunnen verklaren. De verschuiving van bestaande machtsrelaties kunnen als ethisch informatief worden beschouwd t.a.v. het beoordelen van de mate van onwenselijkheid van een ethisch risico.

Voordat het bespreken van individuele ethische risico's aanvangt, dient er te worden opgemerkt dat er in deze voorstudie niet expliciet wordt uitgeweid over de *privacyrisico's* van ethische deurbellen, al zijn deze wel significant. Dit wordt niet gedaan, omdat de *privacyrisico's* reeds welbekend zijn, door bestaande wetgeving worden geadresseerd en door Pels Rijcken zijn getoetst in haar juridische advies. Ook merken wij het bestaan van openbare richtlijnen omtrent privacy en deurbelcamera's op. Beschouw bijvoorbeeld de *Richtlijn camera's bij het eigen huis* van de Autoriteit Persoonsgegevens (AP):

- "stel de camera goed af;
- informeer mensen over de camera;
- bewaar de beelden kort of helemaal niet;
- deel de beelden niet;
- blur (geautomatiseerd) gezichten van voorbijgangers;
- beveilig de camerabeelden;
- respecteer de privacyrechten van de mensen die u filmt."⁸¹

⁷⁸ Thomas Mollema, Joost Wijffels, Marin Beijerbach, Lieke Dom en Joris Joziasse, "Citizens, Surveillance and Sensing Responsibly," *Utrecht University and Responsible Sensing Lab* (2022). https://responsiblesensinglab.org/storage/files/cb8e366f-2e10-4bc2-b6d7-be3a391a0f1e/DRH---PubVersion_Group3_CrowdManagement-DataEthicalConsultation.pdf; Steve Mann, "'Sousveillance': inverse surveillance in multimedia imaging," in *Proceedings of the 12th annual ACM international conference on Multimedia (MULTIMEDIA '04)* (2004): 620–627. <https://doi.org/10.1145/1027527.1027673>.

⁷⁹ Zie Murray Goulden en Lewis Cameron, "The role of mundane resistance in the spectacular failure of the smart home," *Big Data & Society* (2025). <https://doi.org/10.1177/20539517251361120>

⁸⁰ Mollema et al., "Citizens, "Surveillance and Sensing Responsibly."

⁸¹ Autoriteit Persoonsgegevens, "Camera's bij het eigen huis," laatst bijgewerkt op 8 april 2025. <https://www.autoriteitpersoonsgegevens.nl/themas/cameratoezicht/camergebruik-in-en-om-het-huis/cameras-bij-het-eigen-huis>

Wie op zoek is naar goede samenvattingen van de privacyrisico's van slimme deurbelcamera's kan goede startpunten vinden in de voetnoot bij deze zin.⁸² N.B. dat in het vervolg wel een aantal aan privacy gerelateerde ethische risico's worden uitgelicht, losstaand van de privacyrechten van een individu zoals vastgelegd in de AVG/GDPR, namelijk *respect* (in de vorm van geïnformeerde toestemming en controle).

Tot slot een woord vooraf over de structuur van de volgende paragrafen. Hieronder is in elke paragraaf een ethische voorstudie gedaan m.b.t. specifieke ethische risico's. Iedere paragraaf bestaat uit een samenvatting van relevante elementen uit de vakliteratuur, die gezamenlijk een algemene indruk verschaffen van de besproken ethische risico's.

3. Ethische risico's gerelateerd aan informatiebeveiliging

De initiële ethische vraag uit het Plan van aanpak gerelateerd aan informatiebeveiliging (*security*) betrof hoe makkelijk kwaadwillende partijen gebruik kunnen maken van de 'blik van de deurbel'. Het ethische risico dat hier speelt is de *veiligheid van de informatie en situatie van stakeholders*. Dit risico is gerelateerd aan *responsible by design*. Samenvattend betreft het de manifestatie van schadelijke consequenties vanwege een kwetsbaarheid van de informatiebeveiliging van de deurbel. Als *Internet of Things* (IoT) toepassingen, zijn slimme deurbellen namelijk verbonden met het internet. Dat betekent dat ze ook extern benaderd kunnen worden voor het aftappen van datastromen, het hacken van de functies van de deurbel of voor andere soorten manipulatie.⁸³ Op grote schaal worden de deurbellen ingezet, waardoor het web van relaties tussen stakeholders waarmee geïnterfereerd kan worden door een kwade actor zich snel uitbreidt. De veiligheid van de deurbelmodellen die op dit moment worden (en zijn) verkocht vormt daarom een ethisch risico. De risicodragende belanghebbenden zijn t.a.v. dit risico divers. Denk hierbij aan de eigenaren van de deurbel, omwonenden en passanten.

Een studie naar of een Ring deurbel nieuwe IoT-bedreigingen met zich meebrengt, concludeerde dat er in 2023 geen sprake was van openstaande bedreigingen aangaande dit veelgebruikte model, dan wel dat het model geheel nieuwe veiligheidsrisico's introduceert (afgezet tegen een gehele *smart home* situatie).⁸⁴ Er is echter wel reden voor een blijvende waakzaamheid t.a.v. de veiligheid van de digitale deurbellen. Ten eerste omdat geen enkel digitaal systeem niet te hacken valt. Ten tweede omdat er in het afgelopen decennium zorgwekkende voorbeelden zijn geweest van Ring-camera's die gehackt zijn. Een voorbeeld uit 2020 laat zien hoe een kwade actor misbruik kan maken van de positionering van de deurbel: de eigenaren van de camera zijn na een hackactie bedreigd en op een racistische manier verbaal misbruikt.⁸⁵

Verder is een nog belangrijker veiligheidsrisico het op grote schaal lekken of slecht beveiligd lekken van data over deurbel-eigenaren, passanten en omwonenden. Vanwege de in het verleden ondermaatse informatiebeveiliging is het mogelijk dat data over de dagelijkse levenspatronen van deurbel-eigenaren, passanten en omwonenden onrechtmatig in handen van derden is gekomen. Hierbij krijgt het ethisch risico het

⁸² Zie voor een laagdrempelige introductie: S. Keith, "Beware Of The Hidden Risks Of Smart Thermostats and Doorbells," *Privacy Hive Blog* (17 mei 2024). <https://blog.privacyhive.ai/your-home-is-your-sanctuary-not-a-surveillance-zone-beware-of-the-hidden-risks-of-smart-thermostats-and-doorbells/>.

⁸³ David Buil-Gil, Steven Kemp, Stefanie Kuenzel, Lynne Coventry, Sameh Zakhary, Daniel Tilley en James Nicholson, "The digital harms of smart home devices: A systematic literature review," *Computers in Human Behavior* 145 (2023): 107770. <https://doi.org/10.1016/j.chb.2023.107770>. Zie p. 9.

⁸⁴ Arnar Pétursson, "Ethical Hacking of a Ring Doorbell," *MSc Thesis in Computer Science* (KTH Royal Institute of Technology, 2023). <https://www.diva-portal.org/smash/get/diva2:1751192/FULLTEXT01.pdf>.

⁸⁵ Buil-Gil, et al., "The digital harms of smart home devices: A systematic literature review."

karakter van beïnvloeding en het inspelen op vastgelegde data over individuen door derde partijen. (Zie hierover ook §4).

Basismaatregelen die zowel betrekking hebben op de leverancier als de gebruiker van de deurbellen om te voorkomen dat dergelijke situaties zich voordoen, zijn onder andere: het treffen van maatregelen zodat data niet direct toegankelijk middels het internet; het instellen van *multi-factor authentication*; het instellen en onderhouden van firewalls; het weerhouden van de toegang tot de data aan medewerkers en derde partijen; het adequaat versleutelen van de verstuurde datastroom; en het hanteren van een veilig WiFi-wachtwoord.

4. Function creep, onverantwoord hergebruik voor surveillance en inbreuk op digitale autonomie

In deze paragraaf wordt er gereflecteerd op meerdere ethische risico's. Ten eerste is er het ethische risico van *function creep*: "een geleidelijke verschuiving van het doel van de technologie, zoals een verschuiving in de richting van meer opdringerigheid of controle."⁸⁶ Een voorbeeld van *function creep* bij een slimme cameradeurbel zou het aanwenden voor *biometrische categorisatie* kunnen zijn. Een toepassing van deze technologie is geïnformeerd door de *toepassing die ontwikkelaars voor ogen hebben*. Bij het inzetten van deze technologie die nu niet in de verboden categorie van de AI Act valt,⁸⁷ is waakzaamheid nog steeds van toepassing, omdat het oorspronkelijke ontwikkelscenario niet per se rekening hoeft te hebben gehouden met het 'mogelijke kwaad van de toekomst'.⁸⁸ *Function creep* heeft betrekking op het idee van betekenisvolle menselijke controle omdat we het willen kunnen voorkomen en heeft ook betrekking op *responsible by design* omdat de meest risicovolle alternatieve toepassingen bij het ontwerp van de technologie reeds geanticipeerd kunnen worden.

Ondanks dat de slimme deurbelcamera initieel niet voor biometrische categorisatie is bedoeld, kan de camera, of de resulterende datastroom, daar na introductie wel voor wordt gebruikt. Het devies van het AP is, zoals hierboven eerder benoemd is: "blur (geautomatiseerd) gezichten van voorbijgangers". Echter lijkt uit dit voorschrift te volgen dat dit *niet* de default instelling is van iedere cameradeurbel. Daaruit volgt op haar beurt dat er wel degelijk gegevens door het apparaat worden vastgelegd die het doel van biometrische identificatie zouden kunnen dienen. Dit illustreert hoe het risico van de *function creep* richting onverwachtse doeleinden met kwade bedoelingen of nare effecten van kracht is.

Een nog realistischer voorbeeld van *function creep* is het onrechtmatige hergebruik van data. Op voorhand kunnen verschillende vormen van hergebruik geïdentificeerd worden.

1. Ten eerste hergebruik door kwade actoren (zie ook §3 hierboven).

⁸⁶ Centrum voor Ethiek en Gezondheid, *Sensoren in de thuissituatie; de ethiek van e-health deel III*, (2020). <https://www.gezondheidsraad.nl/documenten/adviezen/2020/06/30/sensoren-in-de-thuissituatie>.

⁸⁷ Europese Commissie, "AI Act," <https://artificialintelligenceact.eu/ai-act-explorer/>.

⁸⁸ Arne Berger, Albrecht Kurze, Anreas Bischof, Jesse Joshua Benjamin, Richmond Y. Wong en Nick Merrill, "Accidentally Evil: Questionable Values in Smart Home Co-Design," *Conference on Human Factors in Computing Systems (CHI '23)*, April 23– 28, 2023. <https://doi.org/10.1145/3544548.3581504>. Zie het volgende, tekenende citaat: "We offer "questionable values" as a conceptual shorthand to describe when taken for granted, "good" values for a smart home are violated. We argue that questionable values are 1) afforded by designer's assumptions and fallacies; 2) premediated by existing smart IoT material; 3) normalized by the predominance of technosolutionist narratives, around dominant workplace values, embedding logics of power and dominance into design and engineering. Our proposal is this: We urge designers and engineers to make space for questionable values, to embrace and thus anticipate the spectrum along which heterogenous and homogenous values are contended. Thus empowering designers and engineers to better "look around corners," anticipating tomorrow's concerns and forestalling the worst of their harms."

2. Ten tweede hergebruik door de eigenaren van de cameradeurbel, denk hierbij bijvoorbeeld aan het uploaden op het sociale mediaplatform Neighbors of het delen in een WhatsAppgesprek.
3. Ten derde hergebruik door overheden, zoals Politie, gemeenten of Justitie.
4. Ten vierde de aanbieder van de cameradeurbel, bijvoorbeeld Amazon.

AVG-gerelateerde privacyrisico's spelen voor ieder van de vier groepen. Een ethisch risico gerelateerd aan hergebruik is *niet-proportionele en onrechtmatige, grootschalige surveillance*. Het hergebruik kan hierbij uitgevoerd worden door zowel de aanbieder als door een overheidsorganisatie. Beschouw ter illustratie de beschrijving van Calacci, et al. over de surveillancesituatie in Los Angeles:

...it is impossible to walk around many neighborhoods in Los Angeles without being recorded by a Ring-affiliated device. Over 2,000 law enforcement agencies partner with Amazon Ring, giving these departments unprecedented access to surveillance videos and community networks.⁸⁹

In dit voorbeeld werken overheid en aanbieder samen om grootschalige surveillancemogelijkheden te realiseren. Voor zover bekend is er in Nederland (nog) geen sprake van dergelijke samenwerkingen tussen de Nationale Politie en een aanbieder.

Echter zou de aanwezigheid van meer dan een miljoen (!) surveillanceposities in Nederland wel aanleiding kunnen geven van een *function creep* van een onschuldige toepassing zoals het aannemen van pakketjes op afstand en het communiceren met bezoekers, naar een minder onschuldige toepassing zoals grootschalige surveillance. Eigenaren, omwonenden en passanten worden namelijk op kwetsbare manieren vastgelegd: de herhaaldelijk terugkerende patronen uit hun dagelijks leven kunnen eruit worden afgeleid en gebeurtenissen die bijvoorbeeld als compromitterend kunnen worden geïnterpreteerd worden ook geregistreerd. De surveillant kan in theorie gericht misbruik maken van een data-overzicht over burgers met dergelijke rollen, bijvoorbeeld door gericht in te spelen op patronen waarvan burgers zich wellicht niets eens bewust zijn.

Een nuttig idee dat ons in staat stelt om over dit ethische risico na te denken is de 'surveillance-assemblage'. Denk hierover als het verweven raken van publieke en private actoren, waarbij data over bezoekers, maar ook de straat, burens en passanten, gedeeld worden met commerciële partijen.⁹⁰ Hierbij wordt een aspect van het dagelijks leven gedataficeerd op een manier die tot voor kort niet mogelijk was.⁹¹ De blik van (commerciële) organisaties krijgt een systematische toegang tot de openbare en private ruimten rondom woonadressen.

Tot slot is het waardevol om te reflecteren op een gerelateerd ethisch risico: *inbreuk op de Nederlandse digitale autonomie*. In het kader van slimme deurbelcamera's is hier tot op heden geen onderzoek naar gedaan. Een intuïtie t.a.v. dit ethische risico is dat het zich kan manifesteren als er sprake is van (systematisch) hergebruik van de gelogde data door de aanbieder partij buiten de Europese grenzen en wetgeving om, zonder

⁸⁹ D. Calacci, J. J. Shen, en A. Pentland, "The cop in your neighbor's doorbell: Amazon ring and the spread of participatory mass surveillance," *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2 (2022). <https://doi.org/10.1145/3555125>.

⁹⁰ Binnenlands Bestuur, "Hoogleraar waarschuwt voor 'AI-mateloosheid'" (1 augustus 2025). <https://www.binnenlandsbestuur.nl/digitaal/hoogleraar-waarschuwt-voor-ai-mateloosheid>.

⁹¹ Marc Schuilenburg, "Making Surveillance Public." https://beroepseer.nl/wp-content/uploads/2024/01/verkorte_oratie_marc_schuilenburg_making_surveillance_public.pdf.

dat er hierbij sprake is van een expliciete overeenkomst tussen deze aanbieder en organen van de Rijksoverheid. Het leunen op extra-Europese software- en productleveranciers in het kader van de ontwikkeling, levering en hosting van de cameradeurbel maakt het ethische risico onverminderd relevant. De profiterende partij zou bij dit hergebruik de aanbieder zijn, waarbij de risicodragers de Rijksoverheid en de gedataficeerde burgers zouden zijn. Een contemporaine variant van inbreuk op de Nederlandse digitale autonomie betreft de dataopslag buiten de EU.

Zowel de inbreuk op de digitale autonomie als niet-proportionele en onrechtmatige, grootschalige surveillance zijn gerelateerd aan betekenisvolle, menselijke controle over het hergebruik en de voorwaarden van gebruik van de data van slimme deurbelcamera's.

5. Sociale erosie en mentale gezondheid

Er kan sprake zijn van het ethische risico van sociale erosie doordat men overmatig gaat vertrouwen de deurbelcamera's voor veiligheid, in plaats van op het wederzijdse toezicht van burens. In wat volgt, wordt er stilgestaan bij de verschillende facetten van dit ethische risico en de wederkerige relatie met een ander ethisch risico: de mogelijk negatieve effecten op de mentale gezondheid van burgers. Door de toename van surveillance in het dagelijks leven en het gevoel van de burger in toenemende mate bekeken te worden, treden onwenselijke psychologische gevolgen op.

Allereerst kan er over deze hoofdzakelijk sociale dimensie van de ethische aspecten van het deurbellenvraagstuk worden opgemerkt dat de alomtegenwoordigheid van de deurbel twee surveillance-gerelateerde effecten heeft die ten grondslag liggen aan de veranderingen in sociale dynamieken: (1) normalisering; en (2) softening. Normalisering houdt in dat de praktijk van het surveilleren van de omgeving tot het dagelijks leven gaat behoren: het wordt een routine-activiteit, *die burgers zowel uitvoeren als ondergaan*. Er is sprake van softening wanneer vormen van surveillance minder "zichtbaar en opdringerig" worden.⁹² De blik van de deurbel wordt voor mensen zowel normaal als gemakkelijker te ondergaan dan andere vormen van surveillance.

Geënt op de normalisering en softening werkt een lokaal surveillancenetwerk van deurbelcamera's mogelijk sociale erosie in de hand. Een paar voorbeelden hiervan kunnen behulpzaam zijn bij het verkrijgen van een voorstelling van hoe sociale erosie in werking kan treden.

Het selectieve beeld van de deurbel en de veiligheid van een 'blik op de weg' kunnen een averechts effect hebben. In een artikel van het AMS Institute wordt geobserveerd: "Paradoxically, some users of these doorbells feel less secure. They observe everything happening around their house and discuss it anxiously in neighborhood WhatsApp groups. Their subjective sense of security decreases, while objectively it remains unchanged."⁹³ De perceptie van veiligheidsverlies heeft een sterk effect op de sociale cohesie. Het draagt bij aan een kijk op de buurt als op een omgeving waarin mensen

⁹² Schuilenburg, "Making Surveillance Public"; zie ook: Jamie Field, "Amazon's Ring: How Smart Home Cameras Produce A Consumer Policing Model," *PhD-thesis* (University of Texas, 2023). <https://utd-ir.tdl.org/server/api/core/bitstreams/e5a6d361-d7fd-4099-b9ee-83dc325d53a4/content>.

⁹³ Thijs Turèl, "Smart doorbell cameras pose a danger to our society," AMS Institute (16 januari 2024). <https://www.ams-institute.org/news/smart-doorbell-cameras-pose-a-danger-to-our-society/>. Zie voor een Nederlandse vertaling: Thijs Turèl, "Slimme deurbellen zijn een gevaar voor onze samenleving," *Trouw* (16 januari 2024). <https://www.trouw.nl/opinie/slimme-deurbellen-zijn-een-gevaar-voor-onze-samenleving~b0d84768/>.

niet te vertrouwen zijn en waar 'gevaarlijke vreemdelingen' zomaar kunnen opduiken. Dit werkt volgens sommigen een 'verklingsamenleving'⁹⁴ in de hand waarbij geïsoleerde buurtgenoten angstvallig de vreemde voorvallen in hun buurt documenteren, interpreteren en delen.

Wat is hier precies aan de hand? Onderzoekers naar de effecten van Amazon's Ring deurbel op de Amerikaanse samenleving vermoeden dat er sprake is van een "observers effect": "it may incur on new generations of Americans growing up in neighborhoods that are constantly surveilled", schrijven zij, en dit zou "the potential to perpetuate suburban neighborhood fears" kunnen hebben.⁹⁵ Doordat de technologische middelen om de eigen omgeving op een directere wijze te kunnen controleren d.m.v. surveillance worden (onterechte) angsten omtrent de omgeving versterkt. De mogelijkheid *te kunnen kijken* maakt het in dit geval mogelijk vaker *bevooroordeelde interpretaties te geven aan wat men eerder nooit kon bekijken*.

In een column uit *The Guardian* schrijft Wisemann tekenend:

These pricks of paranoid light that watch them as they walk home, that broadcast a darkened street to their family's phones, that make the world seem suspicious and full of dread simply by capturing a night scene through a fisheye lens, what impact does it have on their understanding of equality, or safety, or identity, or youth? Trust takes time to earn, but falls away in seconds.⁹⁶

Een waarde met de naam 'saamhorigheid', en waarden zoals 'vertrouwen' en 'solidariteit' zijn hier in het geding. De bestaande sociale structuren die het inrichten van het lokale leven a.d.h.v. deze waarden mogelijk maken, zouden wel eens brozer kunnen zijn dan we ons realiseren.⁹⁷ Het is lastig om het argument dat dit burgers meer controle geeft over het dagelijks leven d.m.v. signaleren en communiceren op afstand op te zien wegen tegen de negatieve ethische effecten op saamhorigheid, solidariteit en het onderliggende vertrouwen.

Sociale erosie lijkt gerelateerd aan de effecten op de mentale gezondheid van burgers. Tussen de twee onderwerpen kan een wederkerige relatie worden gelegd. Enerzijds heeft sociale erosie psychologische effecten. Anderzijds leidt een psychologisch effect zoals een paranoïde relatie aangaande de buurt, mogelijk gemaakt door het continu kunnen observeren van de omgeving, tot sociale erosie. Een systematisch vooroordeel, zoals een raciaal vooroordeel of een vooroordeel m.b.t. criminaliteit, kan door de observaties verlopend middels het kanaal van de deurbel, (onterecht) bevestigd worden.

⁹⁴ Privacy First, "De Verklingsamenleving," (16 maart 2024), laatst bijgewerkt op 2 april 2025. <https://privacyfirst.nl/artikelen/de-verklingsamenleving/>.

⁹⁵ Calacci, Shen en Pennland.

⁹⁶ E. Wisemann, "Is it time to ring the alarm on internet door cameras? *The Guardian* (9 februari 2025). <https://www.theguardian.com/world/2025/feb/09/is-it-time-to-ring-the-alarm-on-internet-door-cameras>.

⁹⁷ Zie voor verdieping op het gebied van de manifestatie van door vooroordelen gevoede sociale angsten: Mark Cote, Williams Seymour, Jennifer Pybus en Dalia Mariasin, "A Review on the Risks and Psychological Harms Presented by Consumer IoT Products," (UK Government Department for Science Innovation and Technology, 2023). https://assets.publishing.service.gov.uk/media/672b676dfbd69e1861921c21/A_review_of_the_risks_and_psychological_harms_presented_by_consumer_iot_products_-_Cote_et_al.pdf. Cote et al. schrijven: "Racial Discrimination and Profiling: This is compounded by the fact that Amazon has entered agreements with UK police forces such as in Wiltshire, where police have asked residents to register their doorbells to provide footage when there are burglaries. As Wollaston (2021) reported, these kinds of police partnership can lead to and exacerbate racial discrimination and profiling. For example, in 2019 the US, *Vice* magazine looked at over 100 videos posted on the 'Neighbors app' and the majority were all people of colour and fuel "racial anxieties" (Wollaston, 2021)."

Dit wordt 'confirmatiebias' genoemd: de tendens de eigen vooroordelen bevestigd te zien in toekomstige observaties.

Overgaand op een bespreking van mentale gezondheid, is het allereerst relevant om terug te denken aan de massale surveillance die in de vorige paragraaf is benoemd. De psychologische gevolgen van deurbelcamera's voor eigenaren en omwonenden, door directe interactie met de camera, of indirect gestimuleerd door de deurbellen door de effecten van sociale erosie, zouden kunnen wortelen in bijvoorbeeld (i) het idee dat er sprake is van massasurveillance; (ii) het idee veelvuldig geobserveerd te worden door omwonenden; of (iii) confirmatiebias aan de kant van de observant middels de cameradeurbel.

In een andere column van *The Guardian* was niet sociale erosie, maar de psychologische gevolgen voor eigenaren van de deurbellen het onderwerp. Zo schreef Mahdawi dat "Video doorbell derangement syndrome – the symptoms of which include paranoia, anxiety and a compulsion to snoop on your neighbours – is an alarmingly easy condition to develop".⁹⁸ Deze psychologische conditie zou wijdverbreider kunnen zijn dan men nu zich nu voorstelt, en kan op voorhand beschouwd worden als een katalysator van sociale erosie. Het ethische risico is hier dat psychologische kwetsbaarheid van de eigenaar van de deurbel – de surveillant van de omgeving – hem of haar onbedoeld parten kan gaan spelen. Observatie van de directe omgeving voorkomen (denk aan het verzoek van de AP om de camera niet op de openbare weg te richten) is hierdoor dus van belang. Dit verschilt uiteraard per installatiesituatie van de deurbel.

Zie ook S. A. Snijder, "How smart is your doorbell?" *MSc thesis* (Technische Universiteit Delft, 2024), (<https://resolver.tudelft.nl/uuid:2005fccc-ddc6-4d2d-b05a-c068233752b3>) voor een uitgebreide bespreking van de spanningen in de interactie tussen burgers omtrent slimme deurbelcamera's. Wat relevant is om te benoemen, is dat Snijder beperkende en stimulerende factoren identificeerde voor gesprekken tussen burgers over slimme deurbellen. Beperkende factoren zijn: het hebben van weinig kennis over de werking van de deurbellen; confrontatie vermijdend zijn; de effectiviteit van de deurbellen niet inzien; zich afzijdig en onwetend houden m.b.t. de discussie; weinig om de discussie geven; en niet willen uitdragen een slimme deurbelcamera te hebben. Stimulerende factoren zijn: openlijk kunnen interacteren met de deurbelcamera; er veel last van hebben; blootstelling aan media over slimme deurbelcamera's; het meemaken van een concrete aanleiding (zoals diefstal); het terloops hebben besproken van een deurbelcamera; het goede voorbeeld van anderen kunnen volgen; en een goede relatie hebben met andere buurtbewoners.

6. Respect en het doordenken van (sociale groepen) burgers als stakeholders

In deze laatste paragraaf worden de begrijpelijkheid van de sensor en het ontbreken van 'opt-out' mogelijkheden voor passanten en bezoekers als ethische risico's besproken. Onderliggend aan beide onderwerpen is de waarde 'respect'. Burgers waarderen als stakeholder in de praktijken rondom de cameradeurbel is de eerste stap richting het respecteren van hun waardigheid en hun belangen m.b.t. dit vraagstuk. Dit vertaalt zich naar de twee onderwerpen die betrekking hebben op het respecteren van burgers en hun relatie met de sensor: (1) transparantie omtrent en uitlegbaarheid van de werking van de sensor; en (2) respectvolle opt-out mogelijkheden.

1. *Begrijpelijkheid van de sensor.* De functie van een slimme deurbelcamera hoeft niet voor iedereen voor zich te spreken. Het kan voor een interactor onduidelijk zijn (i) hoe hij of zij in beeld komt; (ii) wat er van hem of haar wordt geregistreerd en bewaard; (iii) met wie communicatie mogelijk is via het apparaat. Het ethische risico is hier dat er sprake is van een epistemische asymmetrie tussen de *observant* (eigenaar, overheid, aanbieder) en het *observandum* (burger). 'Epistemische asymmetrie' wil hier zeggen: in een relatie tussen twee partijen heeft de ene partij kennis die de andere niet heeft, wat kan leiden tot het ontstaan van leed, schade of een kwetsbaarheid bij een van de partijen. In dit geval weet de observerende partij hoe de geobserveerde partij in beeld komt en wordt vastgelegd en hergebruikt. De geobserveerde partij is hier niet van op de hoogte. Van deze asymmetrie kan met name bij kwetsbare sociale groepen effectief misbruik gemaakt worden.⁹⁸

Om dit te verhelpen kunnen er manieren bedacht worden om de interactie tussen burger en sensor te supplementeren met aanvullende uitleg over de werking (het apparaat kondigt dit aan) of door op een andere manier transparant te zijn over waar de sensor toe dient, wat het vastlegt, etc. Het anticiperen op de kennisasymmetrie tussen observeren en geobserveerd worden is een onderwerp dat geadresseerd had kunnen worden middels *responsible by design*.

2. *Respectvolle op-out mogelijkheden.* De slimme deurbelcamera's starten hun werking na ingedrukt te worden of staan permanent te filmen in een stand-bymodus. Echter is er voor de vastlegging van bezoekers en passanten dus geen sprake van een *geïnformeerde toestemming* van de bezoeker of passant. Het ethische risico is hier dus dat er sprake is van een gebrek aan betekenisvolle menselijke controle aan de kant van de bezoeker of passant. Los van de relatie met privacy die dit begrip heeft, kan het uitoefenen van een registratieve actie zonder toestemming van een passant of bezoeker als niet respectvol worden beschouwd. Dit maakt namelijk inbreuk op hun zelfbeschikking. Daardoor is dit een ethisch risico dat zich momenteel op grootschalige basis manifesteert.⁹⁹ Samenvattend: het verkrijgen van toestemming van de bezoeker of passant op een respectvolle manier is benodigd.

Er zijn middelen en (deel)oplossingen voorhanden die betrekking hebben op het mitigeren van dit ethische risico. Denk hierbij bijvoorbeeld aan een *voice assisent* functie die de passant of bezoeker om toestemming vraagt om een opname te starten. Denk ook aan een fysiek middel zoals de Shutterring,¹⁰⁰ een opbouwschuifje voor de cameralens die eerst van de camera afgeschoven moet worden voordat men zichtbaar is. Deze afscherming van het opgenomen worden, beveiligt de zelfbeschikking van de bezoeker of passant over de keuze wel of niet opgenomen te willen worden. Gerelateerd aan het verkrijgen van toestemming is het idee van '*process consent*' ook interessant om te overdenken. Het gaat hierbij om het *vernieuwen* van de geïnformeerde toestemming van de interactor met de deurbel

⁹⁸ Lottelise Torgersen Bergsrud en Abita Vaseeharanathan, "Surveillance in Smart Cities: A Case Study of Ethical Implications for Vulnerable Groups," *MSc Thesis* (Norges teknisk-naturvitenskapelige universitet, 2024). <https://hdl.handle.net/11250/3160931>.

⁹⁹ Zeming Chen, "A study of ethical issues in developing smart-home technologies," *Medium* (28 april 2021). <https://z003.medium.com/a-study-of-ethical-issues-in-developing-smart-home-health-technologies-2ff9f7369fea>.

¹⁰⁰ Responsible Sensing Lab, "Shutterring," (z.d.). <http://responsiblesensinglab.org/nl/projecten/shutterring/>.

gedurende de doorlopende interactie met de deurbel.¹⁰¹ Ook kan men denken aan het blurren van gezichten als default instelling voor de slimme deurbelcamera's of aan het beperken van de reikwijdte van het zicht van de camera tot een minimum (zeg één tot twee meter), waarbij de scherpste van het beeld afneemt naarmate de afstand groter wordt. Een laatste vorm van mitigering heeft betrekking op het verantwoord ontwerpen van wijken. Wanneer er op voorhand wordt nagedacht over de afstand tussen de deur en het begin van de openbare weg, kan er voorkomen worden dat deurbelcamera's passanten onbedoeld kunnen vastleggen.

¹⁰¹ Centrum voor Ethiek en Gezondheid, *Sensoren in de thuissituatie; de ethiek van e-health deel III*.