The Quest for the Effective Protection of the Right to Privacy

Wisman, T.H.A.

2019

document version
Publisher's PDF, also known as Version of record

Samenvatting

In 2009 lanceerde de Europese Commissie het actieplan voor het Internet van Dingen (hierna het 'IvD'). Om de bijdrage van netwerktechnologieën aan de maatschappij te optimaliseren moeten we van een netwerk van computers naar een netwerk van 'onderling gekoppelde objecten', aldus de Commissie. Dit zou de levenskwaliteit van burgers, werkgelegenheid, de creatie van bedrijfsmogelijkheden, groei van de industrie en het concurrerend vermogen van Europa ten goede komen. Het centrale idee achter deze visie is het uitrusten van objecten met ICT waardoor deze vanuit een unieke digitale identiteit autonoom gegevens kunnen communiceren middels netwerktechnologie en eventueel vanaf een afstand kunnen worden aan- of uitgeschakeld. De Commissie is inmiddels gestopt met het beleid rond het IvD in het algemeen, maar is op verschillende beleidsterreinen nog steeds actief. Deze beleidsterreinen betreffen onder andere transport en energie. De Commissie voert beleid en heeft succesvol wetgeving voorgesteld die de verplichting opleggen tot slimme meters in de woning en het eCall-systeem in de auto. Deze ontwikkeling is politiek omstreden, omdat het uitrusten van deze objecten met IvD-systemen gevolgen kan hebben voor de vrijheid waarmee mensen van deze objecten gebruik kunnen maken. Slimme meters kunnen een gedetailleerd beeld geven van iemands privéleven en het eCall-systeem is in staat om het gaan en staan van een burger in zijn of haar auto nauwkeurig in kaart te brengen. Bovendien kunnen deze systemen van een afstand worden aan-of uitgeschakeld. Bij een slimme meter kan de toevoer van stroom op afstand worden uitgezet, een eCall-systeem introduceert een kwetsbaarheid waardoor een auto op afstand kan worden uitgeschakeld.

Het realiseren van deze visie van de Europese Commissie heeft ingrijpende gevolgen voor het recht op privacy en de vrijheid van burgers. Het herverdeelt de macht in het voordeel van bedrijfsleven en overheden ten koste van grondrechten. De Commissie heeft erkend dat privacy een belangrijk onderwerp is dat moet worden geadresseerd, maar in zijn communicaties wordt privacy onder de noemer 'obstakels' geschaard. In de verschillende documenten die de Commissie rond het IvD naar buiten heeft gebracht komt naar voren dat het de zorgen rond privacy beoogt te adresseren met het gegevensbeschermingsrecht. De achterliggende aanname lijkt te zijn dat het gegevensbeschermingsrecht dezelfde reikwijdte en beperkingsvoorwaarden heeft als het recht op privacy. De Commissie heeft echter in zijn communicaties rond 'fundamental rights impact assessments' aangegeven dat het de bescherming van grondrechten belangrijk vindt en dat er voor de interpretatie en toepassing van deze rechten aansluiting moet worden gezocht bij de rechtspraak van het Europese Hof voor de Rechten van de Mens (hierna 'EHRM') en het Hof van Justitie van de Europese Unie (hierna 'HvJEU'). Naar aanleiding van bovenstaande staat in dit proefschrift de volgende onderzoeksvraag centraal:

Hoe wordt het recht op privacy door de Commissie geïnterpreteerd en toegepast binnen het beleid en regulering van verplichte IvD-systemen?

Het recht op privacy en gegevensbeschermingswetgeving

In dit proefschrift is aangetoond dat de Commissie exclusief gebruik maakt van gegevensbeschermingsrecht in het beleid en reguleren rond verplichte Internet van Dingen-systemen (hierna 'IvD-systemen'). Het recht op privacy, zoals vastgelegd in diverse bronnen van EU recht, wordt buiten beschouwing gelaten. In hoofdstuk 3 is aangetoond dat het gegevensbeschermingsrecht beginselen kent die uitkomst kunnen bieden bij het vaststellen van waarborgen en beperkingen aan deze systemen. Toetsing aan principes zoals doelbinding en dataminimalisering stellen de EU wetgever in staat om te voorkomen dat IvD-systemen worden uitgerust met onnodige surveillance functies. Gegevensbeschermingsrecht ziet echter niet op functies die derde partijen in staat stellen om van een afstand een systeem uit te schakelen, of het aanzetten van een sensor voor een ander doel dan waarvoor deze is geïnstalleerd. Het gegevensbeschermingsrecht ziet typisch op transparante relaties die normaalgesproken vrijwillig worden aangegaan. Daarom is het de vraag hoe geschikt dit recht is om te worden toegepast op ICT-systemen die gedwongen in de privé-omgeving van burgers worden geïnstalleerd.

Een ander problematisch aspect van het gegevensbeschermingsrecht is dat het voorziet in open normen die normaliter worden geïnterpreteerd en toegepast door de (verwerkings)verantwoordelijke, kortom de partij die een belang heeft bij het verwerken van persoonsgegevens. Bovendien is het gegevensbeschermingsrecht niet van toepassing op Europese standaardiseringsorganisaties (hierna 'ESOs'), terwijl dit de partijen zijn die de technische voorschriften opstellen waaraan de IvD-systemen dienen te voldoen. Een laatste bezwaar is dat het onwaarschijnlijk is dat de toepassing van het gegevensbeschermingsrecht leidt tot de toetsing van de noodzakelijkheid van de initiële opname en verzameling van gegevens. Dit geldt te meer nu de Commissie het gegevensbeschermingsrecht in zijn communicaties veelal positioneert als een recht op gegevensbeveiliging.

De kneedbaarheid van het concept privacy kan worden teruggevonden in de creativiteit waarmee het EHRM en het HvjEU het recht hierop toepassen op technologische fenomenen. Het recht op privacy is steevast een betrouwbare bron geweest voor rechters om burgers te beschermen tegen de macht van de overheid en het bedrijfsleven. Daarom biedt dit recht een goed uitgangspunt om te bemiddelen tussen de conflicterende belangen die inherent zijn aan het ontwerp van IvD-systemen. De functies die zien op de verwerkingen van persoonsgegevens, de sensoren en de schakelaars, vallen allemaal onder de reikwijdte van het recht op privacy.

Een analyse van de jurisprudentie toont drie factoren die relevant zijn bij het bepalen van de ernst van de inmenging met het recht op privacy die wordt veroorzaakt door de verplichte installatie van deze systemen. Er moet worden gekeken naar de context van de gegevensverwerking, de aard van de gegevens en de mogelijke toekomstige inbreuken die deze systemen faciliteren. Uit de verscheidene communicaties van de Commissie blijkt dat ze beogen dat IvD-systemen zowel het bedrijfsleven als de overheid zullen dienen en de installatie van deze systemen dient dan ook te worden beoordeeld tegen de achtergrond van deze agenda. Deze systemen hebben het vermogen om de omgeving van burgers uit te rusten

met zintuigen, maar de waarnemingen kunnen tegen de burger worden gebruikt. Om dit panoptisch potentieel van IvD-systemen in de kiem te smoren dienen de vereisten die het EVRM en het Handvest van de Grondrechten van de Europese Unie (hierna 'EU Handvest') stellen aan inmengingen met dit recht strikt te worden getoetst. Beoogde functies die een inmenging vormen op het recht op privacy en gegevensbeschermingsrecht moeten in de wetgeving worden vastgesteld, zodat deze een wettelijke basis krijgen. Het vereiste van voorzienbaarheid vereist dat deze inmenging voldoende precies wordt omschreven. De grootschalige inmengingen en mogelijke toekomstige inbreuken op het recht op privacy die worden veroorzaakt door de installatie van deze systemen geven de EU wetgever slechts een beperkte beoordelingsvrijheid. De noodzakelijkheid van iedere individuele functie van een systeem die het recht op privacy beperkt dient daarom strikt getoetst te worden, waardoor er nadrukkelijk aandacht dient te zijn voor de subsidiariteit van een functie. De subsidiariteitstoets stelt de EU wetgever in staat om overbodige functies of een onnodig inbreuk makende uitvoering van functies te adresseren en om te komen tot een ontwerp dat het recht op privacy respecteert. De subsidiariteitstoets is daarom geschikt om de burger te beschermen tegen het gevaar van *purpose- en function creep*, kortom het inzetten van IvD-systemen tegen burgers voor andere doeleinden dan waarvoor ze oorspronkelijk zijn geïnstalleerd.

Dit deel van de rechtspraak van het EHRM en HvJEU raakt ook aan de communicaties van de Europese Commissie omtrent hun impact assessments, een instrument dat ze inzetten voorafgaand aan het opstellen van een wetgevingsvoorstel om de impact op grondrechten vast te stellen. De Commissie stelt in deze communicaties dat de inzet is om de bescherming van de rechten in het Handvest zo effectief mogelijk te maken. Indien een negatieve impact wordt vastgesteld moet de Commissie kijken of dit wel nodig is. Indien deze impact niet kan worden voorkomen is de vraag of en hoe deze kan worden verlicht door middel van concrete waarborgen. Indien een functie een inmenging of mogelijk toekomstige inbreuk mogelijk maakt moet proportionaliteit in de strikte zin worden getoetst, dit betekent dat er een belangenafweging moet worden gemaakt, waarbij het gegeven dat de privacy van alle burgers in EU lidstaten aan de orde is extra gewicht in de schaal legt.

Conflicterende rollen van de Europese Commissie

Eén van de belangrijkste problemen bij het beleid en het reguleren van het IvD ligt in het feit dat de Commissie twee, bij tijd en wijle, onverenigbare rollen heeft. Aan de ene kant is de Commissie de beleidsmaker die een coördinerende, uitvoerende en beheersende taak heeft binnen het beleid rond IvD-systemen. Aan de andere kant wordt de Commissie geacht op te treden als bewaker van de EU-grondrechten die zijn vastgelegd in het EU Handvest. Artikel 7 van het EU Handvest betreft het recht op privacy en dit correspondeert met artikel 8 EVRM. Als beleidsmaker ten aanzien van IvD-systemen onderhoudt de Commissie nauwe contacten met de partijen die een belang hebben bij een milde, of beter nog, afwezige handhaving van grondrechten. Daarbij dient te worden opgemerkt dat de Commissie in een afhankelijke positie kan verkeren ten aanzien van deze partijen die het probeert te betrekken in zijn beleid.

IvD-systemen kunnen worden uitgerust met functies die enerzijds inmengen met het recht op privacy, maar anderzijds warm worden verwelkomd door bedrijfsleven en overheden.

In de pre-wetgevende fase positioneert de Commissie het gegevensbeschermingsrecht als geschikt instrument om zorgen omtrent privacy mee aan te pakken. Het doet dit evenwel op een wijze waarop het beschermende potentieel van dit recht nagenoeg compleet wordt uitgehold, door de substantieve gegevensbeschermingsprincipes buiten beschouwing te laten. Een terugkerend fenomeen in deze communicaties is dat de Commissie beoogt de gegevens die op massale schaal verwerkt kunnen worden te laten gebruiken voor een groot aantal doelen, inclusief doelen die conflicteren met het privacybelang van burgers, hetgeen lijkt op een impliciete afwijzing van het doelbindingsbeginsel. Daarom staan de verwerkingen van persoonsgegevens die de Commissie in haar toekomstvisie voor ogen heeft haaks op deze hoeksteen van het gegevensbeschermingsrecht. Bij het uitvoeren van de impact analyse op de grondrechten, bij zowel slimme meters als eCall, wordt deze lijn doorgezet en worden principes als doelbinding en dataminimalisering niet besproken. De vereisten die voortvloeien uit het recht op privacy worden in deze analyses, in weerwil van de uitgesproken ambities van de Commissie in zijn eerdere communicaties, buiten beschouwing gelaten. De impact assessment is juist een geschikt instrument om vast te stellen welke functies bijzondere aandacht verdienen, waarbij ontwerpbeslissingen kunnen raken aan het recht op privacy, alvorens deze functies en de waarborgen waarmee ze worden omkleedt op te nemen in het wetsvoorstel, of te besluiten om de systemen hier niet mee uit te rusten.

De impact assessment zou een brug kunnen slaan tussen het werk van de Commissie voorafgaand aan de wetgeving, de wetgevingsprocedure zelf en de fase waarin de Commissie verantwoordelijk is voor uitvoerings- en gedelegeerde handelingen (quasi-wetgevende fase). In deze laatste fase onderhandelt de Commissie met ESOs over de ontwikkeling van standaarden waarin technische regels zijn opgenomen die zien op de werking van de IvD-systemen. In deze quasi-wetgevende fase zijn de betrokken instellingen gebonden aan artikel 290 en 291 VWEU en het EU Handvest. In artikel 290 VWEU wordt bepaald dat binnen een wetgevingshandeling de bevoegdheid aan de Commissie kan worden overgedragen om gedelegeerde handelingen vast te stellen van bepaalde *niet-essentiële onderdelen* van de wetgevingshandeling. Het onderscheid tussen essentiële en niet-essentiële onderdelen moet volgens het HvJEU onder andere worden vastgesteld op basis van de politieke gevoeligheid van een onderdeel en of dit onderdeel raakt aan EU-grondrechten. In artikel 291 VWEU wordt de wijze van toekenning van uitvoeringsbevoegdheden aan de Commissie geregeld. Beslissingen ten aanzien van IvD-systemen die een (mogelijke) inmenging met het recht op privacy veroorzaken moeten worden genomen door de wetgever. Wanneer de impact assessment overeenkomstig de ambities van de Commissie zou worden uitgevoerd, kan hierin een inventarisatie worden gemaakt van de fundamentele ontwerpkeuzes die zijn voorbehouden aan de EU wetgever.

Het vaststellen en opstellen van deze onderdelen is daarom ook van belang voor het verdere wetgevingsproces. Het kan dienen als aanknopingspunt voor het Europees Parlement en de Raad om het debat te voeren over het systeemontwerp en binnen welke grenzen de Commissie mag onderhandelen met ESOs om standaarden te laten ontwikkelen. Zo kan er

worden voorkomen dat er in standaarden regels worden vastgelegd die leiden tot inmengingen met het recht op privacy, zonder dat deze bij wet zijn voorzien en zonder dat de Commissie een duidelijke instructie van de wetgever heeft ontvangen waarin deze inmenging nauwkeurig wordt begrensd en omkleed met waarborgen. Als hierover niets wordt geregeld in de basisregeling waarin die de installatie van IvD-systemen verplicht, dan gaat de Commissie de onderhandelingen met de ESOs in zonder een duidelijke instructie over de ontwerponderdelen die raken aan grondrechten. Mocht de Commissie in het verzoek dat het richt aan de ESOs hierover stil blijven, dan is het dus uiteindelijk aan deze organisaties of het uiteindelijke ontwerp van het IvD-systeem zal raken aan de fundamentele rechten. Een dergelijk verzoek van de Commissie aan ESOs, dat ten grondslag ligt aan de ontwikkeling van standaarden door de ESOs, kan door hen geweigerd worden (bijvoorbeeld als er te strenge eisen in zijn opgenomen ten aanzien van gegevensverwerking). Een dergelijke weigering is met het oog op de belangen die worden vertegenwoordigd in ESOs, deze bestaand hoofdzakelijk uit het bedrijfsleven, geenszins denkbeeldig. De Commissie kan in dat geval makkelijker besluiten tegemoet te komen aan de eisen van zijn autonome onderhandelingspartner als de wetgevingshandeling waarin de uitvoeringsbevoegdheid van de Commissie is vastgelegd geen eisen stelt aan het verzoek dat ze aan de ESOs moet doen.

De twee case studies die zijn gedaan in dit boek, in hoofdstuk vijf en zes, tonen aan dat de Commissie in haar impact assessments stil blijft over grondrechten en deze stilte continueert in de verzoeken die worden gedaan aan ESOs. Het verzoek aan de ESOs betreffende de slimme meter stelt slechts dat er *rekening moet worden gehouden* (‘take account of’) met gegevensbeschermingswetgeving. Het verzoek op basis waarvan de standaarden voor het eCall-systeem zijn ontwikkeld noemt het identificeren en adresseren van privacyrisico’s, maar noemt het eCall-systeem niet. Het interpreteren en toepassen van privacy- en gegevensbeschermingswetgeving op specifieke onderdelen van het ontwerp van de verplichte IvD-systemen blijft uit.

Vrijheid, autonomie en architectuur

Vrijheid en autonomie zijn twee belangrijke waarden die het recht op privacy beoogt te beschermen. Gegevensbeschermingsrecht wordt soms vergeleken met milieurecht, omdat het beoogt schadelijke gevolgen van de verwerking van persoonsgegevens te beperken. Het verwerken van persoonsgegevens is in de media wel eens vergeleken met het boren naar olie. Gegevens zijn de grondstof voor tal van processen die een hele industrie dienen. Hoe persoonlijker gegevens zijn en hoe indringender het beeld is dat ze blootgeven van de burgers op wie ze betrekking hebben, hoe schadelijker de gevolgen van verwerkingen zijn voor de vrijheid en autonomie van deze burgers. Beslissingen ten aanzien van het ontwerp van IvD-systemen zijn bepalend voor de vraag of deze systemen schadelijke effecten hebben op onze vrijheid en autonomie. Dit schadelijke effect moet worden vermenigvuldigd met het aantal systemen dat in de EU wordt uitgerold. Dit geeft een idee van de gevolgen van slecht ontworpen systemen. Het recht op privacy geeft de mogelijkheid om de verplichte installatie van deze systemen, de noodzakelijkheid van de functies waarmee zij zijn uitgerust en de

belangenafweging die aan de uitrol ten grondslag ligt, te toetsen. De Commissie heeft gefaald in de uitvoering van deze taak. Nota bene, de Commissie is er niet eens in geslaagd om de exacte problemen vast te stellen die het heeft beoogd op te lossen met de verplichte uitrol van deze systemen.

De inertie van de Commissie staat in scherp contrast met zijn ambities om te komen tot een zo effectief mogelijke bescherming van de rechten in het EU Handvest en zelfs een cultuur te kweken waarin medewerkers die schrijven aan wetsvoorstellen een 'fundamental rights reflex' krijgen. Hoe rechtvaardigt de Commissie het uitblijven van deze reflex bij het opstellen van voorstellen die beogen de privé-omgeving van de burger uit te rusten met ICT, zodat deze kan worden onderworpen aan een publiek-privaat surveillance regime? Dit doet de Commissie door de zorgen omtrent privacy te adresseren met een interpretatie en toepassing van het gegevensbeschermingsrecht waarin het alle substantieve beginselen buiten beschouwing laat, ofwel '*data protection light*'. In deze aanpak worden beginselen zoals doelbinding en dataminimalisering genegeerd en ligt de nadruk op het delen van gegevens waarbij de eisen van vertrouwelijkheid, integriteit en beveiliging centraal staan. Dit zijn eisen die voorwaarden stellen aan de verwerking van gegevens, maar niet geschikt zijn om de noodzakelijkheid van de initiële opname en verzameling van gegevens te toetsen. De Commissie bewijst lippendienst aan het gegevensbeschermingsrecht en zo nu en dan aan het recht op privacy, maar wanneer het aankomt op een toepassing van het recht in overeenstemming met de rechtspraak van het EHRM en het HvJEU blijft het muisstil. De Commissie vertrouwt consequent in alle fases van beleid en regulering in deze benadering van gegevensbescherming-light, waardoor ernstige inbreuken op het recht op privacy worden verpakt in technische termen die een neutrale indruk maken. Dit maskeert het feit dat deze systemen de privé-omgeving van de burger in vergaande mate incorporeert in de immer uitdijende surveillance-staat. De Commissie gebruikt de taal van gegevensbescherming teneinde de gegevens van burgers te onteigenen.

Indien architectuur politiek is, kenmerkt de Europese Commissie zijn beleid en regulering rond verplichte IvD-systemen een gecoördineerde stilte ten aanzien van fundamentele ontwerpbeslissingen. Deze stilte maakt het mogelijk dat deze beslissingen worden genomen door ESOs en dit zal normaliter niet leiden tot beslissingen die de effectieve bescherming van het recht op privacy dienen. De Commissie heeft zowel intern als extern signalen ontvangen over hoe de slimme meter en eCall konden worden ontworpen op een wijze die de privacy van burgers daadwerkelijk zou beschermen, maar hier is niets mee gedaan. Dit heeft geleidt tot een vacuüm in de wetgeving rond het ontwerp van deze systemen. De uiteindelijke beslissingen omtrent gegevensontwerp van IvD-systemen worden buiten de democratische arena genomen. De partijen die hierover beslissingen nemen, vertegenwoordigen niet de burgers van de EU, maar deelbelangen die aanwezig zijn in overheden en bedrijfsleven en die veelal worden vertegenwoordigd door technische experts. De voordelen die uit deze beslissingen worden verwacht dienen de belangen van een relatief kleine groep, terwijl alle burgers in EU lidstaten de negatieve gevolgen zullen ondergaan. Het zal de a-symmetrie in bestaande machtsrelaties alleen maar verder vergroten. Deze praktijk is in strijd met de waarden waar de EU op berust: menselijke waardigheid, vrijheid, democratie, de rechtstaat

en eerbiediging van mensenrechten. Als de Commissie zijn beleid doorzet transformeert de privéomgeving van de burger langzaamaan in een hedendaags digitaal panopticum. Het uiteindelijke ontwerp van deze systemen volgt een logica die zou kunnen worden geduid met *gegevens-onteigening door ontwerp*.

De Commissie is in de beste positie om het huidige beleid grondig te herzien. Het kan door impact assessments de ontwerpbeslissingen in kaart brengen die belangrijk zijn en die aan de basis behoren te liggen van beleid en wetgeving. De architectuur van IvD-systemen gaat alle relevante EU instellingen aan, tenminste als democratie en grondrechten niet slechts zijn bestemd om te functioneren als slogans. De opstelling van surveillance-systemen op een massale schaal waardoor publieke toegang kan worden verschaft tot gegevens over de privésfeer is kenmerkend voor een totalitaire samenleving, de dreiging waarvan onder andere leidde tot het opstellen van het EVRM. Hiermee wordt niet beweerd dat de partijen die deze opdringerige visie ondersteunen dergelijke aspiraties hebben. Totalitaire regimes delen echter wel eigenschappen met deze partijen in het feit dat ze proberen een bepaalde visie op te leggen waarin gedrag, gevoel en verlangen tot in vergaande mate worden gecontroleerd. Wat gebeurt er immers met de burgers die geen boodschap hebben aan deze visie en er graag buiten willen leven? Ongehoorzame burgers, of 'onwillige consumenten' (de Commissie spreekt van 'reluctant consumers') krijgen niet de keuze om buiten het IvD te leven. Iedereen wordt geacht mee te lopen in de parade die de Commissie organiseert tussen de industrieën van transport, energie, mobiele diensten, telecommunicatie en publieke autoriteiten. De burger wordt geacht mee te betalen aan de introductie van zijn eigen digitale dwangbuis. De verplichting om de privésfeer voor deze corporatieve visie open te stellen toont een treffende gelijkenis met de karaktertrekken die Ian Shapiro vaststelt die tegen de essentie van democratische rechtvaardigheid ingaan (zie noot 44 onder 'Conclusion'): 'it is unnecessary, it is not usually entered into voluntarily, it is hard or impossible to escape, it is both a-symmetrical and non-self-liquidating, and it has effects that permeate through the social world.' Het fenomeen dat hij omschreef was slavernij.

Uiteindelijk is het antwoord op de vraag hoe de Commissie het recht op privacy interpreteert en toepast binnen het beleid en regulering van verplichte IvD-systemen tamelijk kort. Niet.