Interoperabiliteitsverplichting voor online messagingdiensten: wapen of bedreiging voor privacy gebruikers?

Een onderzoek de mogelijke implicaties van de interoperabiliteitsverplichting voor online messagingdiensten in artikel 7 DMA voor het recht op privacy van gebruikers

Masterscriptie Informatierecht

Merel Burkunk

Studentnummer: 11213442

E-mail en telefoonnummer: merel.burkunk@student.uva.nl 0624943849

Mastertrack: Informatierecht

Begeleider: Joris van Hoboken

Datum: 6 januari 2023

Aantal woorden: 12979

Beoordeling: 9,0

UNIVERSITEIT VAN AMSTERDAM

Abstract

Interoperability obligation for online messaging services: Weapon or threat to user privacy?

The interoperability obligation for gatekeeping online messaging services under Article 7 DMA carries both positive and negative implications for users' privacy. The purpose of this study is to determine how to provide the greatest possible protection for users' right to privacy when implementing this obligation, specifically with regard to their right to confidentiality of communications and personal data protection.

On the one hand, the interoperability obligation can contribute to stronger safeguards for users' right to privacy. Interoperability reduces the strong network effects and lock-in from which gatekeepers benefit, potentially creating more competition and giving users an actual choice for an alternative online messaging service that offers better privacy protection. Also, interoperability may ensure that online messaging services have a commercial interest in providing the best privacy protection, which may lead to more privacy innovation. In addition, interoperability can lead to more widespread use of end-to-end encryption within the online messaging market and provides an opportunity for the market to choose the most privacy-friendly end-to-end design as a standard.

On the other hand, the interoperability requirement creates a wider exchange of communication data, which puts pressure on the supposedly stronger privacy protection of an alternative interoperable service, especially with regard to data minimization and purpose limitation. It is expected that consent will be used as the basis for this additional personal data processing in the context of interoperability. The risk of pop-up fatigue must then be taken into account.

The implications of the interoperability obligation for end-to-end encryption and security is subject to debate. Some experts believe that interoperability and reliable end-to-end encryption and security cannot go together; others point to technical solutions. Moreover, standardization in the online messaging market may make it harder for online messaging services to make changes to their protocols, which may ultimately lead to stagnation of innovation in privacy protection for users.

The outcome of this tangle of pros and cons will depend heavily on technical (im)possibilities and behavior of users and the market. However, the Commission can adopt guidelines through Article 47 DMA to minimize privacy risks. This would also make it less easy for gatekeepers to invoke these risks purely to evade the obligation. First, in its guidelines, the Commission can advise gatekeepers to request sufficient relevant information from the requesting party on privacy protection. In addition, the Commission can clarify what exactly it understands by data necessary to ensure effective interoperability. Furthermore, it can advise gatekeepers to provide users who communicate via interoperable services with objective just-in-time information about the implications of doing so. The Commission can also recommend that gatekeepers use a certain common standard for end-to-end encryption and service security. In addition, the Commission can clarify in its guidelines that the security level must be ensured even after interoperability is enabled, for example by implementing changes or innovating.

This effort by the Commission through guidelines is crucial to give wing to the interoperability obligation in Article 7 DMA, while ensuring users' right to privacy.

493/500 words

Inhoudsopgave

Hoofdstuk 1. Inleiding

1.1 Probleemstelling

De Europese Digital Markets Act (DMA), die op 1 november 2022 in werking is getreden, bevat in artikel 7 een interoperabiliteitsverplichting voor online messagingdiensten die als zogenaamde 'poortwachter' aangewezen zijn. Dit betekent dat deze poortwachtende diensten berichtenverkeer tussen hun eigen dienst en concurrerende diensten mogelijk moeten maken, als de concurrerende dienst hiertoe een verzoek indient.

Het uiteindelijke doel van deze interoperabiliteitsverplichting is het creëren van een eerlijkere markt.[1] In messagingmarkten ontstaan vaak sterke netwerkeffecten, en dit kan negatieve gevolgen hebben voor de mededinging. Op dit moment wordt de Europese messagingmarkt gedomineerd door slechts twee grote spelers: WhatsApp en Facebook Messenger, beide onderdeel van Meta.[2] Dit gebrek aan concurrentie kan innovatie in de weg staan en bovendien oneerlijke handelspraktijken in de hand werken.[3] Door een interoperabiliteitsverplichting in te voeren, kunnen concurrenten gebruikmaken van het netwerk van deze dominante partijen, waardoor de drempel om effectief te concurreren wordt verlaagd en zij mee kunnen dingen naar een positie op de markt.[4] Gebruikers kunnen dan bijvoorbeeld overstappen naar een concurrerende dienst als Signal, zonder daarmee het gehele WhatsApp-netwerk en daarmee het contact met WhatsApp-vrienden te verliezen.

De interoperabiliteitsverplichting in artikel 7 DMA heeft mogelijk ook belangrijke gevolgen voor het recht op privacy van gebruikers, specifiek het recht op vertrouwelijkheid van de communicatie en persoonsgegevensbescherming, neergelegd in artikelen 7 en 8 Handvest en 8 EVRM.

Enerzijds kan artikel 7 DMA de waarborgen voor het recht op privacy namelijk versterken. Interoperabiliteit op de online messagingmarkt resulteert potentieel in meer keuzevrijheid voor gebruikers, die nu kunnen kiezen tussen verschillende concurrerende diensten met elk een eigen privacybeleid, zonder hun oude netwerk te verliezen.[5] Dit kan positieve gevolgen hebben voor

[1] Impact Assessment DMA, §108-111.
[2] Impact Assessment DMA, §50 en p. 43; Dallal 2022.
[3] Impact Assessment DMA §25-30.
[4] Overweging 64 DMA.
[5] Brown 2020, p. 33; Brown 2022d.

de vertrouwelijkheid van communicatie, specifiek ook het vertrouwen in communicatiediensten en communicatievrijheid[6], en de uitoefening van het recht op persoonsgegevensbescherming. Mogelijk leidt de toename in keuzevrijheid ook tot innovatie op privacygebied.[7]

Anderzijds zorgt de interoperabiliteitsverplichting ook voor een bredere uitwisseling van communicatiegegevens, wat weer risico's met zich meebrengt voor de privacy van gebruikers.[8] Hiernaast bestaan er in de literatuur grote zorgen over de gevolgen van de interoperabiliteitsverplichting voor end-to-end encryptie – indien poortwachters hier gebruik van maken – en beveiliging van online communicatie.[9] Gebrekkige versleuteling en beveiliging zou het recht op privacy van gebruikers onder druk kunnen zetten.

Volgens artikel 7 DMA mag de privacy van gebruikers echter niet lijden onder interoperabiliteit. De vraag is dus in hoeverre bovenstaande positieve en negatieve implicaties bestaan, en op welke manier de grootst mogelijke privacybescherming aan gebruikers kan worden geboden. Het organiseren van interoperabiliteit op een goede manier, zodat zowel mededingingsrechtelijke voordelen worden getrokken als de privacy van gebruikers wordt gewaarborgd, is een zeer complexe klus. Desalniettemin heeft de Europese Commissie middels richtsnoeren de kans om twijfels uit de weg te ruimen en artikel 7 DMA vleugels te geven. De onderzoeksvraag luidt dan ook:

Hoe kan bij de implementatie van de interoperabiliteitsverplichting voor online messagingdiensten in artikel 7 DMA de grootst mogelijke bescherming worden geboden aan het recht op privacy van gebruikers, specifiek het recht op vertrouwelijkheid van communicatie en persoonsgegevensbescherming?

In dit onderzoek is gekozen om het begrip nummeronafhankelijke interpersoonlijke communicatiedienst aan te duiden met het bondigere 'online messagingdienst'.

[6] Zuiderveen Borgesius & Steenbruggen 2019, p. 298-300.
[7] Cyphers & Doctorow 2021, p. 7; Stoltz e.a. 2022.
[8] Barczentewicz 2022, p. 7; EDPB 2020.
[9] Stoltz e.a. 2022.

1.2 Methodiek, deelvragen en leeswijzer

In dit juridisch doctrinair onderzoek evalueer ik eerst de interoperabiliteitsverplichting in artikel 7 DMA vanuit een intern normatief perspectief, namelijk het recht op privacy, en dan specifiek het recht op vertrouwelijkheid van communicatie en persoonsgegevensbescherming. Vervolgens doe ik enkele aanbevelingen waar de Europese Commissie rekening mee kan houden bij het opstellen van eventuele richtsnoeren.

De onderzoeksvraag wordt beantwoord met behulp van de vijf deelvragen. Deelvraag 1 (descriptief) dient als introducerende en definiërende vraag, en luidt: *wat houdt de interoperabiliteitsverplichting voor online messagingdiensten in artikel 7 DMA in?* Hier zal onder meer de definitie worden besproken van begrippen als online messagingdiensten, interoperabiliteit en 'poortwachters' in de DMA, hun samenhang en de relevante problematiek. Deze deelvraag zal in hoofdstuk 2 beantwoord worden.

Deelvraag 2 (evaluerend) schetst de mogelijke positieve gevolgen van de interoperabiliteitsverplichting voor het recht op vertrouwelijkheid van communicatie en persoonsgegevensbescherming, zoals naar voren gebracht in de literatuur en toetsend aan het grondrechtelijk kader. Zij luidt: *hoe kan het doel van artikel 7 DMA, namelijk het creëren van een eerlijkere markt, zorgen voor sterkere waarborgen voor het recht op privacy van gebruikers, specifiek het recht op vertrouwelijkheid van communicatie en persoonsgegevensbescherming?*

Deelvraag 3 (evaluerend) schetst de mogelijke negatieve gevolgen en risico's van de interoperabiliteitsverplichting voor het recht op vertrouwelijkheid van communicatie en persoonsgegevensbescherming van gebruikers, en luidt: *wat zijn de risico's van artikel 7 DMA voor het recht op vertrouwelijkheid van communicatie en persoonsgegevensbescherming van gebruikers?*

De negatieve en positieve gevolgen uit deelvraag 2 en 3 zullen aan bod komen in hoofdstukken 3 t/m 5, elk met betrekking tot een ander deelonderwerp. Op basis van de in deelvragen 1 t/m 3 vergaarde informatie over de risico's van een interoperabiliteitsverplichting worden in deelvraag 4 (ontwerpend) enkele aanbevelingen gedaan. Zij luidt: *welke handvatten kan de Europese Commissie bieden bij het vaststellen van eventuele richtsnoeren ex artikel 47 DMA*

om het recht op vertrouwelijkheid van communicatie en persoonsgegevensbescherming van gebruikers bij de implementatie van artikel 7 DMA maximaal te beschermen?

Met de zinsnede 'onder welke voorwaarden' in de onderzoeksvraag wordt verwezen naar de maatregelen die door de Commissie genomen kunnen worden. De uiteindelijke onderzoeksvraag is dus een ontwerpvraag.

1.3 Het recht op vertrouwelijkheid van communicatie en persoonsgegevensbescherming

Het recht op privacy staat centraal in dit onderzoek, en dan specifiek het recht op vertrouwelijkheid van communicatie en het recht op bescherming van persoonsgegevens. In deze paragraaf volgt een kort overzicht van het juridisch kader dat geldt voor deze twee grondrechten, beperkt tot dat wat relevant is voor dit onderzoek.

1.3.1 Recht op vertrouwelijkheid van communicatie

Communicatie tussen mensen geniet al sinds jaar en dag een speciale bescherming in het recht, beginnend bij het briefgeheim.[10] Inmiddels geldt het recht ook voor moderne communicatietechnologieën, zoals communicatie via online messagingdiensten.[11] Aan het recht op vertrouwelijkheid van communicatie liggen drie waarden ten grondslag.[12] Allereerst beschermt het de individuele privacy: het schermt pottenkijkers af van de persoonlijke gedachten van degene die communiceert. Ten tweede beschermt het recht op vrijheid van meningsuiting, specifiek de communicatievrijheid: wanneer men zeker is dat communicatie vertrouwelijk kan worden gedeeld, voelt men zich vrij om zich te uiten. Dit draagt bij aan het zelfbeschikkingsrecht over communicatie, aan een gevoel van individuele autonomie. Bovendien zorgt het communicatiegeheim ervoor dat men zich niet belemmerd voelt om controversiële meningen en denkbeelden te delen die bijdragen aan het publieke debat.[13] Ten derde is het recht op vertrouwelijkheid van communicatie essentieel voor het vertrouwen in communicatiediensten. Mensen voelen zich alleen vrij om te communiceren als zij erop kunnen vertrouwen dat hun communicatie in veilige handen is en zij bereid zijn om de controle over hun gegevens te verliezen aan aanbieders van communicatiediensten.[14]

[10] Steenbruggen 2009, p. 11, p. 40-42.
[11] Arnbak 2015, p. 133; EHRM 5 september 2017, ECLI:CE:ECHR:2017:0905JUD006149608 (*Bărbulescu v. Romania*), §72 en 74.
[12] Zuiderveen Borgesius & Steenbruggen 2019, p. 298-300.
[13] Steenbruggen 2009, p. 47-48; Zuiderveen Borgesius & Steenbruggen 2019, p. 298-299.
[14] Zuiderveen Borgesius & Steenbruggen 2019, p. 299-300.

Het recht op vertrouwelijkheid van communicatie wordt in het Europees grondrechtelijk kader beschermd door de artikelen 8 EVRM en 7 Handvest: communicatie dient vertrouwelijk te blijven tenzij inmenging in dit recht noodzakelijk is in het belang van verschillende doeleinden, waaronder openbare veiligheid en de bescherming van de rechten en vrijheden van anderen.[15]

Onder het begrip communicatie vallen zowel de inhoud van de communicatie als de bijbehorende verkeersgegevens, ook wel metadata genoemd. De inhoud van communicatie is de letterlijke tekst die wordt gecommuniceerd. Verkeersgegevens zijn gegevens die noodzakelijk zijn voor het overbrengen van communicatie over het netwerk of voor de facturering ervan.[16] Bij communicatie via online messagingdiensten zijn verkeersgegevens bijvoorbeeld de datum en het tijdstip van het versturen van een bericht, en het IP-adres van de verzender en ontvanger.[17]

Traditioneel gold het recht op vertrouwelijkheid van communicatie alleen voor de inhoud van communicatie, en niet voor verkeersgegevens. In de huidige tijd kunnen verkeersgegevens door moderne technieken echter op grote schaal worden verzameld en geanalyseerd en kan hieruit privacygevoelige informatie worden afgeleid.[18] Inmiddels zijn verkeersgegevens ook onder de bescherming van artikel 8 EVRM en 7 Handvest gebracht. Wanneer de verwerking van verkeersgegevens een gedetailleerd inzicht geeft in het leven van mensen, moeten deze aan de hand van dezelfde waarborgen worden geanalyseerd als die welke gelden voor inhoud van communicatie.[19]

Specifiek voor de sector elektronische communicatie ontwikkelde de Europese wetgever de ePrivacy Richtlijn. De ePrivacy Richtlijn is vooralsnog niet van toepassing op online messagingdiensten, hoewel sommige auteurs dit wel aanmoedigen.[20] De ePrivacy Verordening

[15] Council of Europe 2021; Council of Europe e.a. 2019; Kranenborg, in: *The EU Charter of Fundamental Rights: A Commentary* 2014.
[16] Artikel 2(b) ePrivacy Richtlijn.
[17] Zwenne 2018, art. 11.1 Tw, aant. 3; Brown 2022b, §2.1.
[18] Zuiderveen Borgesius & Steenbruggen 2019, p. 315; Van Hoboken & Zuiderveen Borgesius 2015, p. 201.
[19] HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*), §26-27, §39-40; HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2/Watson*), §99; HvJ EU 2 maart 2021, C 746/18, ECLI:EU:C:2021:152 (*Prokuratuur*), §39-40; EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch*), §342 en 363.
[20] Van Hoboken & Zuiderveen Borgesius 2015, p. 198-210; overweging 11 ePrivacy Verordening; Zuiderveen Borgesius & Steenbruggen 2019, p. 313.

zou hier verandering in kunnen brengen, en daarmee de gegevensverwerking ten behoeve van interoperabiliteit nog meer inkaderen.[21]

1.3.2 Recht op bescherming van persoonsgegevens

Naast het grondrecht op vertrouwelijkheid van communicatie wordt communicatie via online messagingdiensten ook beschermd door het recht op bescherming van persoonsgegevens. Dit recht is sinds de jaren 70 in toenemende mate belangrijk geworden binnen de EU-privacyrecht, en is vastgelegd in artikelen 8 EVRM en 8 Handvest.[22] Persoonsgegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet.[23]

Het belangrijkste wettelijke instrument van de EU op het gebied van persoonsgegevensbescherming is de Algemene Verordening Gegevensbescherming (hierna: AVG).[24] Dit onderzoek zal zich met name focussen op de beginselen van dataminimalisatie, doelbinding en integriteit, en de verwerkingsgrondslag toestemming in de AVG.[25]

De AVG kent bovendien een specifieke bescherming toe aan zogenaamde bijzondere persoonsgegevens. Dit zijn gegevens waaruit bijvoorbeeld ras, politieke voorkeur, religie of seksueel gedrag van personen afgeleid kan worden.[26] De inhoud van communicatie kan potentieel dit soort gegevens bevatten en dus deze strengere bescherming genieten.

[21] Brown 2022a, §2.1.
[22] Zuiderveen Borgesius & Steenbruggen 2019, p. 296; Council of Europe 2021; Council of Europe e.a. 2019; Kranenborg, in: *The EU Charter of Fundamental Rights: A Commentary* 2014.
[23] Artikel 8(2) Handvest.
[24] Council of Europe e.a. 2019, p. 34-36
[25] Artikel 5(1)(b), 5(1)(c), 5(1)(f) en 6(1)(a) AVG.
[26] Artikel 9 lid 1 AVG.

Hoofdstuk 2. Interoperabiliteitsverplichting voor online messagingdiensten als oplossing voor poortwachtersproblematiek in de DMA

2.1 Inleiding

In dit hoofdstuk wordt besproken hoe platformmacht in digitale markten kan zorgen voor mededingingsrechtelijke problemen, specifiek ook in de online messagingmarkt. Door bedrijven met een sleutelrol, zogenaamde poortwachters, te reguleren probeert de aankomende Digital Markets Act (DMA) te zorgen voor een eerlijkere markt. Interoperabiliteitsverplichtingen zijn een graag gezien instrument om hieraan bij te dragen. Artikel 7 DMA roept zo'n interoperabiliteitsverplichting in het leven voor poortwachtende online messagingdiensten. Zij worden verplicht om in te gaan op een interoperabiliteitsverzoek van een concurrent, mits voldaan kan worden aan veiligheids- en privacyvereisten. Tot slot wordt in dit hoofdstuk de rol van de Europese Commissie besproken als centrale toezichthouder van de DMA.

2.2 De Digital Markets Act

De Europese Commissie is hard bezig om de Europese Unie klaar te stomen voor het zogenaamde 'digitale tijdperk'.[27] Onderdeel van deze digitale strategie is het ontwikkelen van nieuwe wetgeving die inspeelt op de problemen die zijn ontstaan in onze huidige digitale samenleving en economie. De Digital Markets Act ('Verordening over betwistbare en eerlijke markten in de digitale sector', hierna: DMA) van 14 september 2022 is hier een voorbeeld van.[28]

De DMA speelt in op problemen in de zogenaamde platformeconomie. Het overgrote deel van onze online handel, informatie-uitwisseling en -opslag gaat via steeds groter groeiende online platformen. Het online platform is dé manier voor bedrijven om hun klanten in de Europese Unie te bereiken. Dit is in vele opzichten voordelig voor bedrijven en consumenten en de Europese interne markt als geheel, maar de platformeconomie brengt ook uitdagingen met zich mee voor regulering, met name door gebrek aan concurrentie, oneerlijke handelspraktijken en gefragmenteerd toezicht.[29] De DMA introduceert regels voor platformen die optreden als

[27] 'Europe fit for the Digital Age: new online rules for platforms', ec.europa.eu.
[28] Digital Markets Act.
[29] Impact Assessment DMA, §25-29; Crémer e.a. 2019, p. 19.

zogenaamde poortwachters, om zo een eerlijkere digitale economie te creëren met meer concurrentie op digitale markten.[30]

Inmiddels is het voorstel van de Europese Commissie uit 2020 goedgekeurd en is de DMA op 1 november 2022 in werking getreden. De DMA zal met ingang van 2 mei 2023 daadwerkelijk van toepassing zijn.[31] Poortwachters hebben na een aanwijzingsbesluit door de Commissie zes maanden de tijd om te voldoen aan de verplichtingen van de artikelen 5, 6 en 7 DMA, waaronder de interoperabiliteitsverplichting voor online messaging.[32]

2.3 Platformmacht

In een bloeiende platformeconomie kunnen sommige online platformen buitensporig veel controle en macht uitoefenen, ook wel platformmacht genoemd.[33] In deze paragraaf worden verschillende factoren genoemd die bij kunnen dragen aan platformmacht, onder andere met voorbeelden uit de online messagingmarkt.

2.3.1 Platform als poortwachter

Allereerst kunnen platformen macht uitoefenen in hun rol als tussenpersoon tussen de verschillende gebruikers van een platform. Zo is WhatsApp bijvoorbeeld tussenpersoon voor gebruikers die met elkaar willen communiceren, en verbindt Thuisbezorgd.nl restauranteigenaren aan hongerige klanten. Deze platformen hebben de mogelijkheid om de toegang tot een specifieke eindgebruikersgroep te controleren, en kunnen daarmee als zogenaamde ‘poortwachter’ fungeren tussen eindgebruikers onderling of tussen ondernemingen en hun potentiële klanten.[34]

2.3.2 Netwerkeffecten

Hiernaast kunnen verschillende economische karakteristieken van online platformen bijdragen aan platformmacht. Binnen platformen kunnen allereerst sterke netwerkeffecten ontstaan. Dit houdt in dat de waarde van de dienst toeneemt bij toename van het aantal gebruikers, ook wel ‘direct effect’. Denk hierbij bijvoorbeeld aan sociale media en online messagingdiensten. Hoe meer vrienden WhatsApp gebruiken, hoe aantrekkelijker het wordt om hier zelf ook gebruik

[30] Impact Assessment DMA, §108-111.
[31] Artikel 54 DMA.
[32] Artikel 3(10) DMA.
[33] Busch e.a. 2021, p. 4.
[34] Busch e.a. 2021, p. 5.

van te gaan maken, en hoe groter de drempel wordt om het platform te verlaten. Wanneer er geen mogelijkheid is om te communiceren tussen verschillende diensten, leidt dit ertoe dat je vastzit in het ecosysteem van een platform (*lock-in*).[35]

Verder doen zich vaak indirecte netwerkeffecten voor bij platformmarkten: wanneer het aantal gebruikers groeit, neemt ook de waarde van het platform toe voor ondernemingen die aangesloten zijn op het platform.[36] Steeds meer online messagingdiensten bieden nu speciale functies aan voor zakelijke gebruikers, om rechtstreeks met hun klanten te kunnen communiceren (denk aan WhatsApp Business, Messenger for Business van Facebook, Apple Business Chat en Google Business Messaging).[37] De waarde van bijvoorbeeld WhatsApp Business neemt toe voor ondernemingen als er meer consumenten gebruikmaken van WhatsApp.

Uit deze directe en indirecte netwerkeffecten vloeien ook overstapkosten (*switching costs*) voor gebruikers voort die bijdragen aan de macht van een platform.[38] Dit houdt in dat gebruikers het lastig vinden om als collectief over te stappen naar een nieuw platform, ook wanneer dit nieuwe platform innovatiever of op een andere manier 'beter' is.[39] Het risico bestaat namelijk dat het netwerk van de gebruiker de overstap niet volgt en de gebruiker alleen en ontkoppeld achterblijft op een nieuw platform. Een reeds succesvol platform met een omvangrijk gebruikersbestand heeft hierdoor een grote voorsprong op potentiële concurrenten. Om een kans te maken zullen concurrenten veel tijd en geld moeten investeren om voldoende gebruikers aan zich te binden en zo de toegangsbarrière te doorbreken. Een reguleringsmaatregel als een interoperabiliteitsverplichting kan nieuwe spelers helpen om de markt gemakkelijker te betreden, en daarmee zorgen voor meer concurrentie.[40]

2.3.3 Economies of scale en scope

Verder profiteren online platformen ook geregeld van sterke schaal- en toepassingsvoordelen: *economies of scale* en *economies of scope*. *Economies of scale* is het voordeel dat een platform

[35] Impact Assessment DMA, §80.
[36] Busch e.a. 2021, p. 7-8.
[37] Vermeulen 2021; Winokur Munk 2022.
[38] Busch e.a. 2021, p. 8; Crémer 2019, p. 22-23.
[39] Zie bijvoorbeeld Griggio e.a. 2022 over het onvermogen van WhatsApp-gebruikers om na een wijziging in het privacybeleid over te stappen op een vermeend privacyvriendelijker alternatief, verder besproken in §3.2.
[40] Crémer 2019, p. 22-23, 38.

geniet doordat de hoge initiële productiekosten en vaste kosten van het onderhouden van een platform gepaard gaan met lage of nagenoeg nihil marginale kosten van extra platformgebruikers.[41] Bijvoorbeeld: Google heeft aanvankelijk veel geïnvesteerd in het ontwikkelen van een goed functionerende zoekmachine, maar het toevoegen van een extra gebruiker kost het bedrijf nagenoeg niets, terwijl deze gebruiker wel nieuwe advertentie-inkomsten genereert. De gemiddelde kosten dalen dus aanzienlijk wanneer het gebruikersbestand groeit.[42] Dit geldt bijvoorbeeld ook voor Facebook Messenger, dat een advertentiemodel hanteert.[43]

Door *economies of scope* kan een platform kosten verlagen of de kwaliteit van een dienst verhogen door slim gebruik te maken van reeds voor een andere dienst ontwikkelde middelen en kennis, bijvoorbeeld een bestaand distributienetwerk of de reeds verzamelde gebruikersdata. Zo kan een platform leren van gebruikersgedrag en op basis hiervan een nieuwe dienst ontwikkelen, of een nieuw *machine-learning* algoritme trainen met deze data voor verdere optimalisatie van haar eigen dienst.[44] Amazon kan bijvoorbeeld uit haar gebruikersdata afleiden dat een bepaald stuk kinderspeelgoed erg populair is, en dit vervolgens zelf op de markt brengen voor een lagere prijs. In theorie zou Meta uit berichtenverkeer tussen WhatsApp-gebruikers kunnen afleiden in welke producten consumenten geïnteresseerd zijn, en hiervan advertenties laten zien op Facebook.[45] Een ander voorbeeld uit de messagingmarkt is dat Meta het binnen Facebook opgebouwde vriendenbestand gebruikt om gebruikers met elkaar te verbinden via Facebook Messenger.

2.3.4 Platformmacht ontwricht mededingingsrecht

Door de bovengenoemde karakteristieken van platformen die bijdragen aan platformmacht zijn deze markten gevoelig voor een *winner-takes-all* dynamiek: vaak is er binnen een markt één dominante speler die de gehele markt in handen krijgt. Er vindt dan concurrentie plaats om de gehele markt, en niet meer binnen de markt.[46] In de huidige platformeconomie zijn het grote spelers als Google (Alphabet), Amazon, Facebook (Meta), Apple en Microsoft die de

[41] Busch e.a. 2021, p. 9.
[42] Furman e.a. 2019, p. 32.
[43] 'Advertising on Messenger - Extend your reach and find more customers with Messenger ads.', facebook.com.
[44] Busch e.a. 2021, p. 9.
[45] WhatsApp maakt echter gebruik van end-to-end encryptie om de communicatie te versleutelen, waarover later meer.
[46] Crémer 2019, p. 22-23.

concurrentie binnen de markt belemmeren.[47] Het opkopen van potentiële concurrenten is voor deze grote technologiebedrijven bovendien een populaire strategie om hun dominante positie te behouden.[48]

Hiernaast bestaat het risico dat monopolisten hun machtspositie misbruiken om oneerlijke handelspraktijken toe te passen. Daar komt nog bij dat de regulering van online platformen in de EU op dit moment in grote mate gefragmenteerd is, wat zorgt voor rechtsonzekerheid voor marktpartijen.[49] Dit alles maakt dat het gewone Europese mededingingsrecht niet volstaat om een eerlijke interne markt te bewerkstelligen, en er volgens de Europese Commissie aanvullende regulering nodig is.[50]

2.4 Interoperabiliteit

Een van de reguleringsinstrumenten die bij kan dragen aan een eerlijkere digitale markt is de interoperabiliteitsverplichting voor online messagingdiensten in artikel 7 DMA. In deze paragraaf wordt duidelijk wat interoperabiliteit precies inhoudt, hoe dit mechanisme bij kan dragen aan eerlijke mededinging en wat haar relatie is tot standaardisering.

2.4.1 Interoperabiliteit: algemeen

Interoperabiliteit is in de breedste zin van het woord het vermogen van systemen om met elkaar samen te werken, om met elkaar 'te praten'. Het is een van de grondbeginselen van het internet. Miljarden apparaten over de hele wereld gebruiken dezelfde reeks open protocollen en standaarden om met elkaar te communiceren. Onafhankelijk van het type browser dat je gebruikt, is het als gebruiker mogelijk om elke webpagina te laden die er is. Elke webpagina kan naar een oneindig aantal andere pagina's verwijzen, waardoor een wereldwijd systeem van onderling verbonden data ontstaat.[51]

Ten grondslag aan interoperabiliteit ligt interconnectie: het verbinden van twee of meerdere netwerken.[52] Denk bijvoorbeeld aan de afspraak om alle treinsporen in Nederland dezelfde breedte te geven, waardoor de netwerken van verschillende spoorwegmaatschappijen op elkaar

[47] Moore & Tambini 2018, p. 21-24.
[48] Crémer 2019, p. 110.
[49] Impact Assessment DMA, §37-54.
[50] Overweging 4-5 DMA.
[51] Tarkowski e.a. 2022, p. 12; Cyphers & Doctorow 2020.
[52] Zie de in het Europees wetboek voor elektronische communicatie gebruikte definitie in artikel 2(28) EECC.

aangesloten konden worden. Of aan het verbinden van verschillende telefonienetwerken, zodat het als klant van T-Mobile mogelijk is om te bellen met een klant van KPN. Interoperabiliteit speelt in het bijzonder ook op het dienstenniveau: niet alleen maken interoperabele diensten gebruik van hetzelfde netwerk (bijvoorbeeld het internet), de diensten of applicaties zijn ook onderling op elkaar aangesloten. Een goed voorbeeld is e-mail. Er bestaan verschillende e-maildiensten, die allemaal aangesloten zijn op het internetnetwerk via interconnectie. Door interoperabiliteit op dienstenniveau is het echter ook mogelijk om als Gmailgebruiker een e-mail te sturen naar iemand die Outlook gebruikt. Interoperabiliteit verbindt dus niet alleen netwerken maar ook diensten.[53]

2.4.2 Interoperabiliteit als instrument voor mededinging

De interoperabiliteitsverplichting is in de huidige tijd een graag gezien instrument om dominante platformen te reguleren.[54] De Europese Commissie noemt interoperabiliteit als een belangrijke manier om effectieve competitie op de digitale markt teweeg te brengen.[55] Reeds in 2004 zag de Commissie dat netwerkeffecten een belangrijke barrière vormden voor concurrenten, en verplichtte zij de Amerikaanse techgigant Microsoft op straffe van een hoge boete om (kort gezegd) haar besturingssysteem Windows interoperabel te maken met besturingssystemen van derde partijen. Dit ten behoeve van de eerlijke mededinging.[56] Inmiddels is interoperabiliteit in de EU een veelgebruikt beleidsinstrument dat in verschillende markten wordt toegepast.[57]

Verschillende verenigingen voor digitale rechten zien bovendien het gebrek aan zinvolle interoperabiliteit als een van de belangrijke toegangsbarrières voor concurrenten op de digitale markt.[58] Zeker op markten met sterke netwerkeffecten kan interoperabiliteit essentieel zijn om concurrentie op gang te brengen, wat kan zorgen voor lagere prijzen, een hogere kwaliteit van de dienst en meer innovatie.[59] Sommige auteurs hebben echter kritiek op deze fixatie op interoperabiliteit als een wondermiddel voor marktfalen.[60]

[53] Brown 2020, p. 7-9.
[54] Tarkowski e.a. 2022, p. 14.
[55] Impact Assessment DMA, §277; overweging 64 DMA.
[56] 'Commission concludes on Microsoft investigation, imposes conduct remedies and a fine', ec.europa.eu, 24 maart 2004.
[57] Brown 2020, p. 47-53.
[58] Impact Assessment DMA, Annex 1: Procedural Information, p. 32; Windwehr & Schmon 2020.
[59] Scott Morton e.a. 2021, p. 6-7.
[60] Tarkowski e.a. 2022, p. 14-16.

2.4.3 Interoperabiliteit en messaging: standaardisering

Om interoperabiliteit tussen online messagingdiensten (of bijvoorbeeld mobiele telefoonnetwerken) mogelijk te maken is een sterke integratie nodig tussen de systemen, een zogenaamde 'full protocol' interoperabiliteit. Deze vorm van interoperabiliteit gaat vaak gepaard met standaardisering. Dit komt omdat, zoals in de messagingmarkt, de netwerkeffecten afhangen van gebruikers van alle diensten die er zijn, en verschillende diensten het hierdoor eens moeten worden over een gemeenschappelijke standaard.[61] Denk bijvoorbeeld aan een standaard vorm van end-to-end encryptie waaraan alle interoperabele online messagingdiensten moeten voldoen.

Deze noodzaak tot standaardisering kan er echter ook toe leiden dat innovatie gehinderd wordt, door gebrek aan concurrentie op het gebied van de gestandaardiseerde onderdelen van de dienst.[62]

2.5 Artikel 7 DMA: interoperabiliteitsverplichting voor online messagingdiensten

Ook in de DMA wordt interoperabiliteit door de EU ingezet als reguleringsinstrument. Zo bevat de DMA onder andere interoperabiliteitsverplichtingen voor online zoekmachines, web browsers en virtuele assistenten.[63] Dit onderzoek richt zich op de interoperabiliteitsverplichting voor online messagingdiensten in artikel 7 DMA.

2.5.1 Doel artikel 7 DMA

Volgens de Europese wetgever kunnen poortwachters in de online messagingmarkt door het gebrek aan interoperabiliteit nu gemakkelijk profiteren van sterke netwerkeffecten. Bovendien bieden poortwachters vaak online messagingdiensten aan als onderdeel van hun platformecosysteem (denk aan Facebook Messenger), waardoor de toetredingsdrempels voor alternatieve aanbieders van dergelijke diensten nog hoger worden en de overstapkosten voor eindgebruikers toenemen.[64] Met artikel 7 DMA wil de Europese Commissie ruimte bieden aan concurrenten om de markt te betreden.

[61] Crémer 2019, p. 85; Brown 2020, p. 56.
[62] Brown 2020, p. 25; Crémer 2019, p. 85.
[63] Artikel 6(3) DMA.
[64] Overweging 64 DMA; Impact Assessment, p. 43.

Dat betekent in de praktijk dat een poortwachter als Meta, die als eigenaar van WhatsApp en Facebook Messenger het overgrote deel van de markt in de EU in handen heeft, op grond van artikel 7 DMA een verzoek kan krijgen van een concurrent, bijvoorbeeld Signal, om interoperabel te worden met een van haar diensten. Hierdoor wordt er berichtenverkeer tussen de twee diensten mogelijk.

2.5.2 Nummer(on)afhankelijke interpersoonlijke communicatiediensten

Artikel 7 DMA is van toepassing op de zogenaamde 'nummeronafhankelijke interpersoonlijke communicatiedienst', die in dit onderzoek wordt aangeduid met het bondiger 'online messagingdienst'. Dit begrip stamt uit het Europees wetboek voor elektronische communicatie (hierna: Europees wetboek). Hierin wordt onderscheid gemaakt tussen berichtenverkeer via over het internet aangeboden communicatiediensten, ook wel online messagingdiensten (bijvoorbeeld WhatsApp, Facebook Messenger en Signal), en het traditionele sms-berichtenverkeer dat gaat via de mobiele netwerken die worden beheerd door telecommunicatiediensten als KPN en T-Mobile. Beide typen communicatiediensten zijn 'interpersoonlijk': ze maken berichtenverkeer tussen twee of meerdere personen mogelijk. Maar in tegenstelling tot het sms-verkeer zijn online messagingdiensten 'nummeronafhankelijk'. Dat houdt in dat zij niet afhankelijk zijn van een telefoonnummer en dus geen onderdeel zijn van de openbaar toegewezen nummervoorraden.[65] Je hebt bijvoorbeeld geen telefoonnummer nodig om Facebook Messenger te gebruiken, en bij WhatsApp is je 06 slechts een identificatiemethode.

Nummeronafhankelijke interpersoonlijke communicatiediensten zijn pas sinds 2021 onder de reikwijdte van het Europees wetboek gebracht. Net als bij het voorstel voor een ePrivacy Verordening kwam dit voort uit een discussie over het groeiende belang van deze over het internet aangeboden diensten voor de communicatie (zie §1.3.1). Verschillende bepalingen uit het Europees wetboek zijn inmiddels dus ook van toepassing op online messagingdiensten, waardoor er sprake is van gedeeltelijke overlap tussen deze wet en artikel 7 DMA. Zo biedt het Europees wetboek lidstaten reeds de mogelijkheid om in gerechtvaardigde gevallen een interoperabiliteitsverplichting op te leggen aan online messagingdiensten.[66] Dit houdt echter slechts een mogelijkheid in voor lidstaten en is geen directe verplichting voor poortwachters zoals wel in artikel 7 DMA is vastgelegd. Voor dit onderzoek zijn met name de in het Europees

[65] Overwegingen 17-18 en artikel 2(5) en 2(7) Europees wetboek voor elektronische communicatie.
[66] Artikel 61(2)(c) Europees wetboek voor elektronische communicatie.

wetboek vastgelegde definities van telecommunicatiebegrippen van belang. De gevolgen van overlap tussen het Europees wetboek, de DMA en potentieel de ePrivacy Verordening voor online messaging zijn mogelijk interessant om in een toekomstig onderzoek te bespreken.[67]

2.5.3 Poortwachterscriterium

De interoperabiliteitsverplichting in artikel 7 DMA richt zich specifiek op zogenaamde poortwachters. Om binnen de reikwijdte van dit begrip en dus dit artikel te vallen, moet voldaan zijn aan een drietal vereisten.[68] Allereerst moet de poortwachter een wezenlijke impact hebben op de Europese interne markt. Deze impact wordt bijvoorbeeld aangenomen als een platform een zeer grote omzet in de Unie heeft en in ten minste drie lidstaten platformdiensten levert. Ten tweede moet een poortwachter een zogenaamde kernplatformdienst aanbieden in de EU die voor zakelijke gebruikers een belangrijke toegangspoort is om eindgebruikers te bereiken.[69] Online messagingdiensten zijn volgens de DMA te kwalificeren als kernplatformdienst.[70] Tot slot moet een poortwachter een verankerde en duurzame positie hebben in haar activiteiten, of moet deze positie te verwachten zijn in de nabije toekomst. Verder geldt voor ondernemingen die bepaalde financiële drempels halen dat zij op basis daarvan al voldoen aan de poortwachtersvereisten.[71]

Op dit moment domineert het techbedrijf Meta als eigenaar van Facebook app, Facebook Messenger, Instagram en WhatsApp de markt voor online messaging.[72] WhatsApp was in januari 2022 met zo'n 2 miljard gebruikers de meest gebruikte messagingdienst wereldwijd.[73] Ook in de EU staat WhatsApp met stip bovenaan als meest gebruikte messagingdienst, met Facebook Messenger als grote nummer twee.[74] Voorbeelden van messagingdiensten die naar verwachting onder de interoperabiliteitsverplichting voor poortwachters zullen vallen zijn: WhatsApp, Facebook Messenger, Instagram Direct Message, Apple's iMessage, Android Messages en Microsoft's Skype. Voorbeelden van kleinere messagingapps die er hoogstwaarschijnlijk buiten vallen zijn Signal en Telegram.[75]

[67] Zie hierover BEREC 2021.
[68] Artikel 3(1) DMA.
[69] Artikel 3(1) jo 1(2) DMA.
[70] Artikel 2(2)(e) DMA.
[71] Artikel 3(2) DMA.
[72] Van Dijck e.a. 2019, p. 7.
[73] Dixon 2022; Griggio e.a. 2022, p. 2.
[74] Dallal 2022.
[75] Stoltz e.a. 2022; Brown 2022b.

2.5.4 Voorwaarden artikel 7 DMA

Volgens artikel 7 DMA moeten poortwachtende online messagingdiensten op verzoek van een concurrent de basisfuncties van hun dienst interoperabel maken met de concurrent in kwestie, en hiertoe de nodige technische interfaces aanbieden.[76]

Voor het recht op privacy van gebruikers is van belang dat het veiligheidsniveau, met inbegrip van end-to-end encryptie, dat de poortwachter aan zijn eigen eindgebruikers biedt, volgens artikel 7 DMA te allen tijde behouden moet blijven. Bovendien moet de poortwachter een referentieaanbod publiceren met de technische details en algemene voorwaarden van interoperabiliteit met haar dienst. Indien een poortwachter die gebruik maakt van end-to-end encryptie (zoals WhatsApp) dus een verzoek krijgt van een partij die hier geen gebruik van maakt, kan deze het verzoek afwijzen. Interoperabiliteit moet in principe binnen drie maanden na een verzoek geregeld zijn door de poortwachter. Het moet gebruikers echter altijd vrijstaan om wel of niet gebruik te maken van de interoperabele functies.[77]

Ook relevant voor de privacy van gebruikers is dat de poortwachter en verzoeker alleen persoonsgegevens met elkaar mogen delen die strikt noodzakelijk zijn om effectieve interoperabiliteit te bieden. Bovendien mag de poortwachter maatregelen nemen om ervoor te zorgen dat verzoekers de integriteit, veiligheid en privacy van haar diensten niet in gevaar brengen, mits deze maatregelen proportioneel zijn.[78]

2.6 Rol Europese Commissie

In de DMA is de voorkeur gegeven aan gecentraliseerde handhaving op EU-niveau, anders dan gedecentraliseerde handhaving op nationaal niveau. Dat wil zeggen dat de Europese Commissie in de eerste plaats toezicht houdt op de poortwachters. Dit staat in schril contrast met de Europese gewoonte om wetgeving op EU-niveau uit te vaardigen, maar te laten handhaven door nationale autoriteiten.[79] Toch is voor dit centrale toezicht gekozen, met name omdat de problemen in digitale markten waaraan de DMA het hoofd wil bieden een grensoverschrijdende aard hebben. Bovendien is er een zeer beperkt aantal poortwachters dat onder de DMA valt, en

[76] Zie Appendix voor details artikel 7 DMA en bijbehorende overweging 64.
[77] Artikel 7(3-5, 7) DMA.
[78] Artikel 7(8-9) DMA.
[79] Larouche & De Streel 2021, p. 558-559.

hebben zij allemaal een pan-Europees of zelfs mondiaal bereik. Om deze redenen is centraal toezicht volgens de Commissie dus het efficiëntst.[80]

Naast vele andere bevoegdheden, waaronder het opleggen van sancties, kan de Commissie op grond van artikel 47 DMA eventueel richtsnoeren vaststellen voor alle onderdelen van de DMA om de effectieve uitvoering en handhaving ervan te vergemakkelijken.[81] Dit geldt dus ook voor de interoperabiliteitsverplichting uit artikel 7 DMA. Bovendien kan de Commissie de hulp inschakelen van Europese standaardisering-instellingen, en hen verzoeken om technische standaarden te ontwikkelen die interoperabiliteit vergemakkelijken.[82]

2.7 Tussenconclusie

Nu uitvoerig uiteen is gezet wat de interoperabiliteitsverplichting voor online messagingdiensten in artikel 7 DMA inhoudt, en welke problematiek deze beoogt op te lossen, zullen in hoofdstuk 3 t/m 5 de potentiële gevolgen van deze verplichting voor het fundamentele recht op privacy van gebruikers worden besproken. Vervolgens worden op basis hiervan in hoofdstuk 6 enkele aanbevelingen gedaan voor richtsnoeren ex artikel 47 DMA.

[80] Impact Assessment DMA, §102–107 en 192.
[81] Zie ook overweging 95 DMA.
[82] Artikel 48 DMA.

Hoofdstuk 3. Keuzevrijheid tussen online messagingdiensten door interoperabiliteit kan privacywaarborgen versterken

3.1 Inleiding

In dit hoofdstuk wordt beargumenteerd hoe de interoperabiliteitsverplichting voor online messagingdiensten in artikel 7 DMA kan zorgen voor meer keuzevrijheid voor gebruikers, en daarmee de waarborgen voor het recht op privacy kan versterken. Een interoperabiliteitsverplichting kan namelijk de door sterke netwerkeffecten veroorzaakte gebruiker *lock-in* waar poortwachters nu van profiteren verminderen, en daarmee de drempels om de markt te betreden verlagen. Hierdoor hebben gebruikers een daadwerkelijke keuze tussen verschillende diensten met elk hun eigen privacybeleid, en kunnen zij bijvoorbeeld kiezen voor een privacyvriendelijker alternatief. Bovendien kan meer keuzevrijheid zorgen voor een groter vertrouwen in communicatiediensten en bijdragen aan communicatievrijheid. Hiernaast maakt keuzevrijheid dat gebruikers 'vrijelijker' akkoord kunnen gaan met privacyvoorwaarden, zoals vereist in de AVG. Tot slot kan een interoperabiliteitsverplichting innovatie op het gebied van privacy stimuleren, omdat diensten door toename van mededinging op de markt een commercieel belang hebben om de beste privacybescherming aan te bieden.

Bij deze mogelijk positieve gevolgen worden in dit hoofdstuk echter ook enkele kanttekeningen geplaatst, met als belangrijkste het risico dat gebruikers de communicatie van interoperabele partijen zullen weigeren op grond van artikel 7 lid 7 DMA. Dit kan bovenstaande privacyvoordelen ondermijnen en bovendien ingrijpende gevolgen hebben voor de praktische uitwerking van de interoperabiliteitsverplichting in het algemeen.

3.2 Keuzevrijheid door interoperabiliteit: reacties in de literatuur

In de huidige online messagingmarkt die gedomineerd wordt door poortwachter Meta, zouden sommige gebruikers vanuit privacyoverwegingen graag willen overstappen naar een concurrerende online messagingdienst. Door de sterke netwerkeffecten en hoge overstapkosten (zie §2.3.2) slagen zij hier echter zelden in.

In 2021 kondigde WhatsApp bijvoorbeeld een fundamentele aanpassing in haar privacybeleid aan, waardoor er onder andere op grotere schaal gegevens van WhatsApp-gebruikers gedeeld zouden gaan worden met Meta. Hierop installeerden WhatsApp-gebruikers massaal de

messagingapps van vermeend privacyvriendelijkere concurrenten.[83] Signal kreeg er in één maand 20 miljoen nieuwe gebruikers bij, en Telegram zo'n 90 miljoen.[84] In een onderzoek naar de gebeurtenis gaf 25% van de ondervraagden aan vanwege het nieuwe privacybeleid te willen overstappen naar een andere messagingapp. Uiteindelijk is slechts een kwart van hen dit gelukt. 0,52% van het totale aantal ondervraagden heeft de WhatsApp applicatie verwijderd. De belangrijkste reden hiervoor was volgens ondervraagden de sterke netwerkeffecten: gebruikers konden een groot deel van hun netwerk niet bereiken vanuit de nieuwe messagingapp, en vielen daardoor weer terug op WhatsApp.[85]

Een interoperabiliteitsverplichting voor online messaging zou deze sterke netwerkeffecten kunnen verminderen en zorgen voor meer concurrentie op de markt (zie ook §2.2). Zoals uit bovenstaand voorbeeld blijkt kan dit ook invloed hebben op de keuzevrijheid die gebruikers hebben ten aanzien van messagingapps en het privacybeleid dat zij voeren. Door interoperabiliteit kunnen gebruikers die door privacyoverwegingen zijn overgestapt naar een kleinere, alternatieve applicatie namelijk alsnog hun oude netwerk bereiken. Wel moet opgemerkt worden dat de keuze om interoperabel te worden altijd bij de kleinere messagingdienst zal liggen en deze niet vanzelfsprekend geïnteresseerd hoeft te zijn in interoperabiliteit met een poortwachter (zie hierover §4.5). In dit hoofdstuk wordt echter uitgegaan van de hypothetische situatie dat de diensten wel interoperabel willen worden.

De Electronic Frontier Foundation (EFF), een non-profit organisatie die opkomt voor burgerlijke vrijheden in de digitale wereld, stelt zelfs dat meer concurrentie ervoor zal zorgen dat ondernemingen onder druk worden gezet om betere gastheren te zijn, uit angst dat gebruikers zullen overstappen.[86] Specifiek zorgt een interoperabiliteitsverplichting er volgens EFF voor dat gebruikers gemakkelijk een dienst met ongunstige privacyvoorwaarden kunnen verlaten, en dat dominante platformen daadwerkelijk kunnen worden gestraft voor het niet respecteren van de privacy van gebruikers.[87]

Ian Brown, hoogleraar Informatiebeveiliging en Privacy en expert op het gebied van interoperabiliteit, wees ook op deze potentieel positieve gevolgen van een

[83] Griggio e.a. 2022, p. 1–23.
[84] Newton 2021.
[85] Griggio e.a. 2022, p. 1–23.
[86] Cyphers & Doctorow 2021, p. 7; Stoltz e.a. 2022.
[87] Cyphers & Doctorow 2021, p. 24.

interoperabiliteitsverplichting voor privacy. Gebruikers hebben nu een 'daadwerkelijke keuze' om gebruik te maken van een bepaalde messagingdienst, onder andere op basis van de mate van privacy die deze dienst biedt.[88] Het wordt dan makkelijker voor nieuwe, privacy-gefocuste concurrenten om de markt te betreden.[89] Of zoals een andere auteur zegt: mededinging kan consumenten helpen te kiezen voor privacy.[90] Ook het Centre on Regulation in Europe (CERRE) stelt in een rapport dat het beschermen van de privacy een motivatie kan zijn voor een interoperabiliteitsverplichting, omdat innovatie en concurrentie bevorderd worden en gebruikers de mogelijkheid krijgen hun gegevens beter te controleren.[91]

Bovendien wijst het Impact Assessment van de DMA zelf ook op deze potentieel positieve gevolgen voor de privacy van gebruikers. Volgens de Commissie zal het aanpakken van oneerlijke handelspraktijken van poortwachters bijdragen aan meer keuze voor de consument wat betreft het aantal platforms dat innovatieve en privacyvriendelijke diensten aanbiedt.[92] Gebrek aan concurrentie tussen verschillende platformen zorgt namelijk voor lagere kwaliteit en een hogere 'prijs' voor consumenten.[93]

3.3 Keuzevrijheid door interoperabiliteit: bezien in privacyrechtelijk kader

Deze argumenten uit de literatuur kunnen als volgt gekoppeld worden aan het eerder geschetste kader voor het recht op privacy, specifiek het recht op vertrouwelijkheid van communicatie en persoonsgegevensbescherming:

3.3.1 Keuzevrijheid geeft ruimte aan privacyvriendelijk alternatief

Allereerst kan de mogelijkheid om te kiezen voor een privacyvriendelijker alternatief ervoor zorgen dat er minder verkeersgegevens verzameld worden. Voorbeelden van vermeend privacyvriendelijke alternatieven zijn de online messagingdiensten Signal en Telegram. Signal profileert zich als hét privacyvriendelijke alternatief voor WhatsApp. Signal is een onafhankelijke non-profit organisatie en is niet door eigenaarschap verbonden met een van de dominante technologiebedrijven, anders dan WhatsApp dat onderdeel is van Meta.[94] Net als WhatsApp gebruikt Signal end-to-end encryptie om de inhoud van communicatie te

[88] Brown 2020, p. 33; Brown 2022d.
[89] Brown 2022b.
[90] Alexander 2021, p. 1.
[91] Bourreau e.a. 2022, p. 40.
[92] Impact Assessment DMA, §337.
[93] Impact Assessment DMA, §66.
[94] O'Flaherty 2021.

versleutelen (zie ook §5.2.1), maar Signal beweert hiernaast een betere bescherming aan de bijbehorende verkeersgegevens te bieden. Anders dan WhatsApp versleutelt Signal ook je profielinformatie en –foto, en weet het niet met wie je communiceert en of je lid bent van een bepaalde groepsapp.[95] Een voorbeeld van een bekende Signal-gebruiker is klokkenluider en privacyvoorvechter Edward Snowden.[96]

De online messagingdienst Telegram slaat anders dan Signal wel contactgegevens, contacten en de user-ID op. Maar dit is nog steeds aanzienlijk minder dan WhatsApp, dat onder andere accountinformatie, contacten, status, betalingen, device-informatie, locatie, cookies, advertentiegegevens en user-ID verzamelt. Hiernaast gebruikt Telegram geen standaard end-to-end encryptie om de inhoud van communicatie te versleutelen, maar is dit wel een optie in zogenaamde 'beveiligde chats'-functie.[97]

Wanneer dit soort privacyvriendelijkere diensten door de interoperabiliteitsverplichting terrein winnen op de messagingmarkt, kan dat er uiteindelijk dus voor zorgen dat er minder verkeersgegevens van gebruikers worden verzameld. Dit draagt bij aan de bescherming van het recht op vertrouwelijkheid van communicatie. In de jurisprudentie van het EHRM en HvJEU wordt namelijk steeds grotere waarde gehecht aan het beschermen van verkeersgegevens, omdat deze een gedetailleerd beeld kunnen geven van iemands privéleven.[98] Verwerking hiervan moet dus worden beperkt tot het strikt noodzakelijke. Bovendien draagt een verminderde verzameling van verkeersgegevens bij aan het beginsel van dataminimalisatie in de AVG, een uitwerking van het recht op persoonsgegevensbescherming.[99]

3.3.2 Keuzevrijheid draagt bij aan vertrouwen in communicatiediensten en communicatievrijheid

Onderzoekers Zuiderveen Borgesius en Steenbruggen noemden het vertrouwen in communicatiediensten en communicatievrijheid als twee van de waarden die ten grondslag liggen aan het recht op vertrouwelijkheid van communicatie (zie §1.3.1).[100] De mogelijkheid

[95] Patel 2022.
[96] O'Flaherty 2021.
[97] Vegelien 2019; 'Privacybeleid van WhatsApp', whatsapp.com, 14 november 2022; 'Telegram Privacy Policy', telegram.org, 8 september 2022.
[98] Digital Rights Ireland, §26-27; Tele2/Watson, §99; Prokuratuur, §39-40; Big Brother Watch, §342 en 363.
[99] Artikel 5(1)(c) AVG.
[100] Zuiderveen Borgesius & Steenbruggen 2019, p. 298-300.

voor gebruikers om onafhankelijk van hun netwerk te kunnen kiezen voor een bepaalde messagingdienst met bepaalde privacyvoorwaarden, zorgt mogelijk ook voor een groter vertrouwen in communicatiediensten in het algemeen. Wanneer mensen autonoom kunnen kiezen voor een in hun ogen privacyvriendelijke messagingdienst, hebben zij wellicht meer vertrouwen dat hun communicatie in veilige handen is, en voelen zij zich bovendien vrijer om te communiceren. Deze keuzevrijheid kan hiernaast bijdragen aan het gevoel van zelfbeschikking over je communicatie: jij bepaalt met welke voorwaarden je akkoord gaat en aan wie je jouw gegevens toevertrouwt. Aansluitend bij deze waarden zou een interoperabiliteitsverplichting de waarborgen voor het recht op vertrouwelijkheid van communicatie enerzijds dus versterken.

Anderzijds blijkt uit onderzoek dat interoperabiliteit tussen messagingdiensten ook een inmenging in het zelfbeschikkingsrecht over communicatie kan betekenen.[101] Het kan gebruikers namelijk de keuze ontnemen om specifieke sociale groepen te scheiden. Zo gaven respondenten aan dat zij bang waren dat relaties die verder van hen afstaan, zoals collega's, hun nu berichten zouden gaan sturen binnen een ecosysteem dat voor hen bedoeld was voor hechtere relaties, zoals familie en naasten. Denk aan een collega die vanuit WhatsApp een bericht stuurt naar jouw Instagram account. Het gevoel dat 'iedereen je overal kan bereiken' werd door sommige respondenten gezien als een inmenging in de privésfeer. Artikel 7 lid 7 DMA verzekert echter dat het gebruikers in alle gevallen vrij moet staan te beslissen om wel of niet van de interoperabele functies gebruik te maken, dus ook om een bericht van buitenaf te ontvangen.

3.3.3 Kanttekening: zelfbeschikking gebruiker als wapen tegen interoperabiliteit

Een beroep op de uitzondering in artikel 7 lid 7 DMA kan echter ook negatieve gevolgen hebben voor het vertrouwen in communicatiediensten en de communicatievrijheid van de verzender. Stel, je wilt vanuit Signal een bericht sturen naar een familielid op WhatsApp, maar deze persoon weigert interoperabele berichten van Signal te ontvangen. Je hebt dan geen zekerheid dat je bericht aankomt, en zal bovendien toch moeten uitwijken naar WhatsApp om je familielid te bereiken. In dat geval profiteert de poortwachter weer van sterke netwerkeffecten en is de verzender niet meer vrij in zijn keuze voor een alternatieve dienst als Signal.

[101] Arnold e.a. 2020, p. 11; Arnold e.a. 2017, p. 11-12.

Bovendien bestaat het risico dat poortwachters deze weigering in de hand werken door de manier waarop zij gebruikers informeren over interoperabele berichten. Zo kan WhatsApp het familielid uit bovenstaand voorbeeld door middel van een pop-up waarschuwen voor de risico's van interoperabiliteit voor effectieve bescherming van zijn persoonsgegevens (zie daarover hoofdstuk 4), en hem stimuleren om het bericht van Signal te weigeren. Een gebruiker die bezorgd is over zijn privacy kan extra gevoelig zijn voor dit soort berichtgeving.

De door artikel 7 lid 7 DMA aan gebruikers gegarandeerde zelfbeschikking kan daarmee ook zwaarwegende gevolgen hebben voor de praktische uitwerking van de interoperabiliteitsverplichting zelf. Wanneer gebruikers massaal berichten van interoperabele diensten weigeren, blijven de sterke netwerkeffecten van kracht en de gebruikers *locked-in* binnen de dienst van de poortwachter. Dit zou op gespannen voet staan met het doel van artikel 7 DMA, namelijk het creëren van een eerlijkere markt, en hindert bovendien de in dit hoofdstuk geprezen toename in keuzevrijheid tussen verschillende diensten voor de gebruiker.

3.3.4 Keuzevrijheid draagt bij aan 'vrijelijk' gegeven toestemming

Buiten deze kanttekening is er een derde mogelijk positief gevolg van de toename in keuzevrijheid tussen verschillende online messagingdiensten voor de privacy van gebruikers. Keuzevrijheid kan namelijk bijdragen aan de door de AVG vereiste 'vrijelijk' gegeven toestemming voor de verwerking van persoonsgegevens.[102] Om een messagingapplicatie te kunnen gebruiken, geven gebruikers toestemming voor de verwerking van hun persoonsgegevens en gaan zij akkoord met bepaalde privacyvoorwaarden (zie §4.4.3). In de huidige markt hebben gebruikers echter nauwelijks een daadwerkelijke keuze om wel of niet toestemming te geven, omdat zij nou eenmaal afhankelijk zijn van bijvoorbeeld WhatsApp om het overgrote deel van hun netwerk te bereiken. Vermindering van sterke netwerkeffecten door een interoperabiliteitsverplichting draagt bij aan de vrijheid om toestemming te geven, omdat gebruikers onafhankelijk van hun netwerk de keuze kunnen maken voor een bepaalde messagingdienst met bepaalde privacyvoorwaarden.

Wel blijft de zogenaamde *pop-up fatigue* een probleem: mensen gaan gemakkelijk akkoord met privacyvoorwaarden, omdat zij vaak geen zin hebben om deze te lezen en door willen met het

[102] Artikel 6(1)(a) jo 4(11) AVG.

gebruiken van de applicatie.[103] Of toestemming daadwerkelijk 'vrijelijk' wordt gegeven is ook hiervan afhankelijk.

3.3.5 Keuzevrijheid leidt tot innovatie op privacygebied

Meer concurrentie betekent vaak meer innovatie.[104] Een laatste mogelijk positief gevolg voor de privacy van gebruikers is dat de toename aan concurrentie op de online messagingmarkt en de daarmee ontstane keuzevrijheid voor gebruikers kan leiden tot meer innovatie op het gebied van privacy. Zoals uitgelegd in hoofdstuk 2 kan het door interoperabiliteit makkelijker worden voor nieuwe, privacy-gefocuste concurrenten om de markt te betreden. Dit kan concurrentie op het gebied van privacyvoorwaarden in de hand werken: poortwachters kunnen immers niet achterblijven als gebruikers massaal vanuit privacyoverwegingen overstappen naar de concurrent. Dit kan leiden tot een commercieel belang bij de bescherming van gebruikersrechten.[105] Andersom krijgen poortwachters bij gebrek aan mededinging de ruimte om niet te hoeven innoveren, en kunnen zij de kwaliteit van de dienst – waaronder privacybescherming – verminderen zonder daarmee gebruikers te verliezen.[106]

Overigens gaat deze redenering ervanuit dat consumenten privacybescherming als doorslaggevende factor zien in de keuze voor een bepaalde dienst. Er bestaat echter ook een mogelijkheid dat online messagingdiensten door het ontstaan van eerlijke mededinging zullen concurreren op prijs.[107] Wanneer de diensten geld gaan kosten, kunnen gebruikers er om die reden juist voor kiezen om in te leveren op privacy en bijvoorbeeld gebruik te maken van een 'gratis' messagingdienst met een verdienmodel dat berust op de analyse van gebruikersgegevens.

[103] Bravo-Lillo e.a. 2014.
[104] Brown 2020, p. 548.
[105] Tarkowski e.a. 2022, p. 14; Scott Morton e.a. 2021, p. 4.
[106] Scott Morton e.a. 2019, p. 34.
[107] Impact Assessment DMA §332, p. 98.

Hoofdstuk 4. Privacygevolgen van bredere uitwisseling communicatiegegevens door interoperabiliteit tussen online messagingdiensten

4.1 Inleiding

Interoperabiliteit tussen online messagingdiensten zal zorgen voor een bredere uitwisseling van inhoud van communicatie en bijbehorende verkeersgegevens. Dit hoofdstuk schetst de mogelijke negatieve gevolgen hiervan voor het recht op vertrouwelijkheid van communicatie en persoonsgegevensbescherming. Bredere uitwisseling van communicatiegegevens zal in de praktijk met name de vertrouwelijkheid van verkeersgegevens onder druk zetten. Verder heeft het mogelijk negatieve gevolgen voor de beginselen van dataminimalisatie en doelbinding in de AVG. Bovendien zullen online messagingdiensten naar verwachting toestemming als verwerkingsgrondslag kiezen bij interoperabiliteit, waarbij het risico op *pop-up fatigue* in acht moet worden genomen. Overigens kan bredere gegevensuitwisseling slecht afstralen op online messagingdiensten die propageren 'privacyvriendelijk' te zijn.

4.2 Waarborgen in DMA bij bredere uitwisseling (verkeers)gegevens

Waar eerst één dienst toegang had tot inhoud van communicatie en bijbehorende verkeersgegevens van gebruikers, hebben door interoperabiliteit twee (of meerdere) interoperabele diensten toegang tot de communicatiegegevens die van de ene naar de andere dienst worden gestuurd. Dit brengt volgens verschillende auteurs risico's voor de privacy van gebruikers met zich mee.[108] De DMA speelt in op deze risico's door te stellen dat de poortwachter en verzoeker alleen persoonsgegevens met elkaar delen die strikt noodzakelijk zijn om effectieve interoperabiliteit te bieden, rekening houdend met de regels in de AVG en ePrivacy Richtlijn.[109] Verschillende privacyvoorvechters onderschrijven dit streven.[110] Hiernaast mag de poortwachter volgens de DMA maatregelen nemen om ervoor te zorgen dat verzoekers de integriteit, veiligheid en privacy van haar diensten niet in gevaar brengen, mits deze maatregelen proportioneel zijn.[111]

[108] Brown 2020, p. 35-39; Barczentewicz 2022, p. 3-8; Cyphers & Doctorow 2021, p. 27-28; Scott Morton e.a. 2021, p. 29.
[109] Artikel 7(8) DMA.
[110] Cyphers & Doctorow 2020; Cyphers & Doctorow 2021, p. 30; EDPB 2020, p. 2-4.
[111] Artikel 7(9) DMA.

4.3 Bredere uitwisseling (verkeers)gegevens en vertrouwelijkheid van communicatie

Wat voor gevolgen heeft de bredere gegevensuitwisseling voor het recht op vertrouwelijkheid van communicatie? Indien de interoperabele diensten gebruikmaken van end-to-end encryptie zal de inhoud van communicatie versleuteld zijn (zie §5.2.1). De bredere uitwisseling van inhoud van communicatie heeft in dat geval dan ook geen negatieve gevolgen voor de vertrouwelijkheid van communicatie van gebruikers, mits de encryptie onaangetast blijft (zie ook §5.2.3). Verkeersgegevens zijn daarentegen meestal niet versleuteld. En dit is ook niet altijd wenselijk: sommige verkeersgegevens zijn essentieel in het succesvol overbrengen van de communicatie van de ene naar de andere dienst, en spelen bovendien een rol bij de bestrijding van spam, phishing en andere vormen van misbruik van de dienst.[112]

Het EHRM en HvJEU benadrukken dat indien verkeersgegevens een gedetailleerd beeld geven van iemands leven, deze moeten worden geanalyseerd aan de hand van dezelfde waarborgen als die welke gelden voor inhoud van communicatie.[113] Bij een bredere uitwisseling van alleen verkeersgegevens omwille van interoperabiliteit moet dus altijd het recht op vertrouwelijkheid van communicatie worden gerespecteerd: inmenging in dit recht is enkel toegestaan wanneer dit noodzakelijk is in een democratische samenleving. De bredere uitwisseling van verkeersgegevens moet dus proportioneel zijn en er moeten voldoende waarborgen tegen misbruik bestaan.[114]

4.4 Bredere uitwisseling (verkeers)gegevens en persoonsgegevensbescherming

4.4.1 Inleiding

In deze paragraaf wordt besproken welke eisen het recht op persoonsgegevensbescherming stelt aan de bredere uitwisseling van gegevens in het kader van interoperabiliteit. De AVG beoogt dit recht te waarborgen en is een zeer omvangrijk instrument. Het bevat veel normen die mogelijk eisen kunnen stellen aan de verwerking van gegevens op grond van artikel 7 DMA. Het rapport *Interoperability for competition regulation* pleit zelfs voor het ontwikkelen van nieuwe AVG-regels specifiek gericht op verwerkingen van persoonsgegevens door derde partijen in het kader van interoperabiliteit.[115] Omwille van de beperkte omvang van dit

[112] Brown 2022b.
[113] Digital Rights Ireland, §26-27; Tele2/Watson, §99; Prokuratuur, §39-40; Big Brother Watch, §342 en 363.
[114] Zuiderveen Borgesius & Steenbruggen 2019, p. 302-303.
[115] Brown 2020, p. 36.

onderzoek zal in het bijzonder aandacht worden besteed aan de beginselen van dataminimalisatie en doelbinding, en de verwerkingsgrondslag toestemming in de AVG. Er wordt aangenomen dat online messagingdiensten persoonsgegevens verwerken, en dat zij in het kader van interoperabiliteit aan te merken zijn als gezamenlijk verwerkingsverantwoordelijken, waardoor er bepaalde verplichtingen uit de AVG voor hen gelden.[116] Verder wil ik aanstippen dat interoperabiliteit ook risico's kan meebrengen voor het uitoefenen van datarechten uit de AVG, zoals het recht op verwijdering, rectificatie en inzage van gegevens.[117] In welke mate interoperabele partijen verwerkingsverantwoordelijke zijn en waar en hoe deze rechten dus kunnen worden uitgeoefend, is mogelijk interessant voor toekomstig onderzoek.

4.4.2 Dataminimalisatie en doelbinding

Artikel 7 lid 8 DMA beperkt de gegevensverwerking tot dat wat strikt noodzakelijk is voor de interoperabiliteit. Hiermee wordt tegemoetgekomen aan het beginsel van dataminimalisatie in de AVG: verwerking van persoonsgegevens moet beperkt worden tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Bovendien mogen gegevens volgens de AVG ook niet langer worden bewaard dan nodig.[118] De European Data Protection Board (EDPB) adviseert interoperabele partijen hiertoe om een gemeenschappelijk niveau van gegevensbeperking en een gemeenschappelijke gegevensbewaringstermijn te overwegen.[119]

Dataminimalisatie hangt samen met het doelbindingsbeginsel: persoonsgegevens moeten voor bepaalde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. Deze doeleinden moeten bovendien welbepaald en uitdrukkelijk omschreven zijn.[120] Ze kunnen dus niet te breed worden geformuleerd.

In de context van gegevensuitwisseling door interoperabiliteit tussen online messagingdiensten moeten deze doeleinden dus duidelijk vastgelegd worden. Daarbij is het van belang te weten welke gegevens precies 'strikt noodzakelijk' zijn voor het doel 'effectieve interoperabiliteit' ex artikel 7 lid 8 DMA, en hoe lang het nodig is om deze gegevens te bewaren. Is interoperabiliteit

[116] Artikel 2(1), 4(7) en 26 AVG.
[117] Brown 2020, p. 36-37; EDPB 2020, §16.
[118] Artikel 5(1)(e) AVG.
[119] EDPB 2020, §17.
[120] Artikel 5(1)(b) AVG.

al ‘effectief’ wanneer puur de overdracht van communicatie heeft plaatsgevonden? Of moet dan ook de beveiliging van communicatie geregeld zijn? En hoe lang moeten gegevens hiervoor bewaard worden, en door wie? Dit zijn begrippen die mogelijk nog verduidelijkt kunnen worden om gegevensbescherming beter te waarborgen.

4.4.3 Toestemming als grondslag

Wanneer persoonsgegevens worden verwerkt moet dit volgens de AVG ‘rechtmatig’ gebeuren, wat inhoudt dat er een grondslag moet zijn voor de verwerking.[121] Omdat communicatiegegevens soms ook te kwalificeren zijn als bijzondere persoonsgegevens (zie §1.3.2), zullen online messagingdiensten in de praktijk veelal gebruikmaken van toestemming als grondslag.[122] Dit houdt in dat gebruikers nadat zij een messagingapplicatie hebben gedownload, de vraag krijgen of zij toestemming geven voor de verwerking en akkoord gaan met de privacyvoorwaarden van de dienst. In deze voorwaarden staat onder andere welke gegevens worden verwerkt, voor welke doeleinden, met wie de gegevens potentieel worden gedeeld, en hoe lang zij worden bewaard.[123] Om in de context van interoperabiliteit te zorgen voor een rechtmatige verwerking zullen de online messagingdiensten opnieuw toestemming moeten vragen aan gebruikers, en wel voor de nieuwe verwerkingen die zullen plaatsvinden door communicatie-uitwisseling met een andere dienst. Toestemming moet volgens de AVG onder andere vrijelijk en geïnformeerd worden gegeven.[124]

Dit zou bijvoorbeeld kunnen in de vorm van een pop-up wanneer een gebruiker een bericht probeert te versturen naar iemand buiten het ecosysteem van de dienst. Hier staat dan een waarschuwing dat deze andere dienst meer verkeersgegevens verzamelt dan de eigen dienst, en dat de gebruiker hier eerst toestemming voor moet geven.[125] Op deze manier wordt informatie over de verwerking verstrekt op het moment dat het voor gebruikers van belang is, een zogenaamde *just-in-time* informatieverschaffing. Dit geeft de gebruiker direct inzage in de gevolgen van de verwerking, zodat zij een geïnformeerde keuze kunnen maken.[126] Toestemming kan ook in de vorm van een algemene wijziging in het privacybeleid van de dienst, waar alle gebruikers mee akkoord moeten gaan om de dienst te blijven gebruiken. Dit

[121] Artikel 6 AVG.
[122] Artikel 9(2)(a) AVG; Brown 2020, p. 38.
[123] Artikel 13 AVG.
[124] Artikel 4(11) AVG.
[125] Zie bijvoorbeeld Hodgson 2022a, onder ‘Talking to Bob’.
[126] FTC 2013, p. 15-16.

zou echter op gespannen voet staan met artikel 7 lid 7 DMA, dat verzekert dat het gebruikers in alle gevallen vrij moet staan te beslissen om wel of niet van de interoperabele functies gebruik te maken.

Onderzoeker Barcezentewicz wijst op het risico dat *pop-up fatigue* een rol gaat spelen bij interoperabiliteit: gebruikers willen simpelweg toegang tot de dienst, en zijn wellicht niet bereid genoeg tijd en moeite te investeren om te ontdekken wat de gevolgen hiervan zijn voor de bescherming van hun persoonsgegevens. Hierdoor bestaat het risico dat gebruikers toestemming geven voor interoperabiliteit in een mate die hen later kan verrassen, zelfs wanneer de messagingdienst alle nodige informatie verschaft.[127] Uit het eerder aangehaalde onderzoek naar WhatsApp (zie ook §3.2) bleek dat een derde van de deelnemers die überhaupt op de hoogte was van de fundamentele wijzigingen in het privacybeleid deze na drie maanden nog steeds niet had gelezen.[128] Het staat dus ter discussie of we dan wel kunnen spreken van een 'geïnformeerde' toestemming, en daarmee een geldige verwerkingsgrondslag.

Een andere mogelijkheid voor een rechtmatige verwerking door interoperabele online messagingdiensten is een beroep op een 'verdere verwerking', verenigbaar met het oorspronkelijke doel.[129] Dit hangt af van welk doel de gebruiker aanvankelijk akkoord mee is gegaan, en hoe dit zich verhoudt tot het nieuwe doel, namelijk interoperabiliteit. Verenigbaarheid is ook afhankelijk van verschillende andere factoren, waaronder de aard van de gegevens, de gevolgen voor de gebruiker en het bestaan van passende waarborgen. Communicatiegegevens zijn mogelijk ook bijzondere gegevens, en dus gevoelig van aard (zie §1.3.2). De gevolgen voor de gebruiker zijn bijvoorbeeld het delen van zijn/haar/hun gegevens met een nieuwe, derde partij, die er een minder strikt privacybeleid op nahoudt. Bovendien is verenigbaarheid afhankelijk van het aantal passende waarborgen dat is genomen, zoals het versleutelen van de inhoud van communicatie, en waar mogelijk de verkeersgegevens. Kijkend naar deze factoren brengt een beroep op verenigbaarheid in veel situaties ernstige risico's met zich mee voor de gebruiker, en is opnieuw toestemming vragen naar mijn mening een veiligere, privacyvriendelijkere optie. De EDPB stelde bovendien eerder al met betrekking tot interoperabiliteit dat er altijd extra toestemming moet worden gevraagd voor de verwerking.[130]

[127] Barczentewicz 2022, p. 7.
[128] Griggio e.a. 2022, p. 13.
[129] Artikel 6(4) AVG.
[130] EDPB 2020, §12.

Samenvattend legt de AVG de verwerking van verkeersgegevens (en inhoud van communicatie) door interoperabele partijen flink aan banden. EFF vindt in haar rapport over privacy en interoperabiliteit aansluiting bij deze AVG-vereisten. Er mogen volgens EFF niet meer gegevens verzameld worden dan noodzakelijk voor interoperabiliteit, en de verzamelde gegevens mogen niet voor secundaire doeleinden te gelde worden gemaakt of geëxploiteerd. Bovendien moeten beide partijen nagaan of zij de geïnformeerde toestemming van de gebruiker hebben voordat zij persoonsgegevens beginnen door te geven. Dataminimalisatie en toestemming zijn volgens EFF de twee leidende principes die gegevensmisbruik moeten voorkomen en controle geven aan de gebruiker.[131]

4.5 Privacy als marketingstrategie

Mits zo goed mogelijk rekening is gehouden met de bovengenoemde beginselen en waarborgen, is de bredere gegevensuitwisseling door interoperabiliteit privacyrechtelijk gezien legaal. Vanuit reputatie- en marketingoverwegingen kunnen bedrijven echter alsnog bedenkingen hebben bij interoperabiliteit. Voor online messagingdiensten die veel waarde hechten aan de vertrouwelijkheid van gegevens van hun gebruikers en deze betrouwbaarheid ook willen uitstralen als organisatie, kan het van groot belang zijn dat hun gebruikers ondanks interoperabiliteit met een derde partij een gelijkwaardige privacybescherming blijven genieten.[132] Wanneer 'hét privacyvriendelijke alternatief' Signal bijvoorbeeld een verzoek tot interoperabiliteit bij poortwachter WhatsApp zou indienen, zou het willen nagaan hoe WhatsApp precies met gegevens omgaat, om aan gebruikers te kunnen verzekeren dat hun gegevens nog steeds veilig zijn. Andersom zou WhatsApp ook een verzoek tot interoperabiliteit af kunnen wijzen als zij denkt dat de privacy van haar eigen gebruikers niet meer gewaarborgd kan worden.

Moxie Marlinspike, oprichter van Signal, wijst op de tegenstelling dat interoperabiliteit gebruikers enerzijds keuzevrijheid geeft om te kiezen met wie ze hun verkeersgegevens willen delen (zie hierover hoofdstuk 3), maar anderzijds ervoor zorgt dat deze verkeersgegevens via een omweg toch weer terechtkomen bij derde partijen die de gebruiker juist wilde omzeilen.[133] Recenter benadrukte de nieuwe CEO van Signal in een tweet dat Signal anders dan WhatsApp geen banden heeft met dominante techbedrijven en geen verkeersgegevens verzamelt over je

[131] Cyphers & Doctorow 2021, p. 30.
[132] Bourreau e.a. 2022, p. 41; Brown 2020, p. 37-38.
[133] Marlinspike 2016.

profiel, met wie je communiceert of aan welke groepsapps je deelneemt.[134] Uit deze trots lijkt door te schemeren dat voor Signal een interoperabiliteitsverzoek aan WhatsApp voorlopig nog niet op de planning staat.

[134] Whittaker 2022.

Hoofdstuk 5. End-to-end encryptie, beveiliging en standaardisering bij interoperabele online messaging

5.1 Inleiding

Dit hoofdstuk bespreekt welke gevolgen artikel 7 DMA zal hebben voor het gebruik van end-to-end encryptie in de online messagingmarkt, en daarmee voor de privacy van de gebruiker. Enerzijds kan interoperabiliteit zorgen voor grootschaliger gebruik van end-to-end encryptie, en biedt het de messagingmarkt de kans om het privacyvriendelijkste end-to-end ontwerp als gemeenschappelijke standaard te kiezen. Anderzijds bestaan er onder sommige experts zorgen over mogelijke risico's van een interoperabiliteitsverplichting voor end-to-end encryptie en beveiliging. Bovendien kunnen online messagingdiensten door standaardisering mogelijk minder makkelijk wijzigingen in hun protocollen doorvoeren, wat uiteindelijk kan zorgen voor stagnatie van innovatie op het gebied van privacywaarborgen voor gebruikers.

5.2 End-to-end encryptie

5.2.1 End-to-end encryptie in online messaging

Sommige online messagingdiensten maken gebruik van end-to-end encryptie om de communicatie van hun gebruikers 'eind-tot-eind' te versleutelen. Bij end-to-end encryptie wordt de communicatie versleuteld op het eigen apparaat van de verzender en vervolgens ontsleuteld op het apparaat van de ontvanger. Dit betekent dat de inhoud van communicatie tijdens transmissie onleesbaar is voor derden die de informatie onderscheppen. Zelfs de online messagingdienst zelf kan de communicatie niet lezen.[135]

End-to-end encryptie is een manier van versleutelen die afgelopen tijd een hoge vlucht heeft genomen, onder meer door de Snowden onthullingen die zorgden voor een groeiende belangstelling voor het waarborgen van de vertrouwelijkheid van communicatie.[136] Onder andere WhatsApp, Facebook Messenger, Signal en Telegram maken gebruik van end-to-end encryptie om de inhoud van berichten te versleutelen. Facebook Messenger en Telegram bieden dit echter alleen aan binnen een speciale 'beveiligde chat'-omgeving. Signal gebruikt end-to-end encryptie ook om sommige verkeersgegevens te versleutelen (zie §3.3.1).

[135] ARTICLE 19 2020, p. 49.
[136] Bagloni e.a. 2016, p. 244.

5.2.2 End-to-end encryptie ligt politiek gevoelig

Dat communicatie via online messagingdiensten end-to-end versleuteld is, is niet vanzelfsprekend. Overheden zetten techbedrijven al jaren onder druk om toegang te krijgen tot de communicatiegegevens van gebruikers. Zij willen net als bij communicatie via traditionele telecomproviders de mogelijkheid krijgen om deze gegevens voor opsporingsdoeleinden te onderscheppen, bijvoorbeeld bij de bestrijding van terrorisme of kinderporno.[137] Bij het ontwikkelen van nieuwe standaarden voor end-to-end encryptie is er dus veel druk vanuit overheden om een zogenaamde 'achterdeur' in te bouwen, waardoor zij alsnog toegang kunnen krijgen tot de versleutelde communicatie. Ook de Commissie zelf heeft recentelijk een voorstel gedaan om de verspreiding van illegale content (i.e. kinderporno) tegen te gaan: een plan dat volgens critici hand in hand gaat met een gedwongen achterdeur in de end-to-end encryptie van online messagingdiensten. Een achterdeur maakt de systemen volgens experts echter kwetsbaarder voor onrechtmatige toegang, bijvoorbeeld door criminelen of buitenlandse inlichtingendiensten. Dit kan de vertrouwelijkheid van communicatie aantasten. Online messagingdiensten verzetten zich dan ook hevig tegen overheden die wensen mee te kijken in de communicatie van hun gebruikers.[138]

5.2.3 End-to-end encryptie van chatgeschiedenis in de cloud

Bij end-to-end encryptie wordt de communicatie van gebruikers tijdens transmissie versleuteld, en wordt de chatgeschiedenis alleen lokaal opgeslagen op de telefoon van de verzender en ontvanger. In de praktijk wordt de chatgeschiedenis echter ook vaak als reservekopie opgeslagen in de cloud. Belangrijk om te vermelden is dat deze reservekopieën niet vanzelfsprekend end-to-end versleuteld zijn. In dat geval heeft de beheerder van de cloud alsnog toegang tot de opgeslagen communicatie.

WhatsApp en Facebook Messenger bieden gebruikers de mogelijkheid om ook hun reservekopie end-to-end te versleutelen, maar dit is geen standaardinstelling. Apple had aanvankelijk wel plannen om deze mogelijkheid aan te bieden voor de opslag van iMessage communicatie in de iCloud, maar staakte dit plan in 2021 na gesprekken met de FBI. Dit zou namelijk negatieve gevolgen hebben voor bewijsvergaring.[139] Recentelijk heeft Apple echter

[137] Bouma 2019; 'VS wil uitstel encryptieplannen Facebook', nos.nl.
[138] Van Dijk 2022; Hijnk & Wassens 2022; Warofka 2022; Endeley 2018.
[139] Afonin 2021.

aangekondigd deze functie in 2023 toch aan te gaan bieden.[140] Gebruikers zullen de mogelijkheid krijgen om hun gehele iCloud reservekopie, waaronder communicatiegegevens, end-to-end te versleutelen. Voor Androidgebruikers was dit al mogelijk.[141] Signal zegt binnen iOS elke mogelijkheid tot opslag buiten het apparaat onmogelijk te hebben gemaakt, waardoor je de Signal chatgeschiedenis überhaupt niet binnen een iCloud reservekopie kan opslaan.[142]

5.2.4 End-to-end encryptie draagt bij aan privacy

End-to-end encryptie draagt bij aan de bescherming van het recht op privacy van gebruikers. De vertrouwelijkheid van communicatie wordt immers gewaarborgd door de end-to-end versleuteling hiervan, en bovendien kan encryptie bijdragen aan de door de AVG vereiste 'integriteit en vertrouwelijkheid' bij persoonsgegevensverwerking: verwerkingsverantwoordelijken zijn verplicht om een passend beveiligingsniveau te waarborgen. Hiertoe schatten zij de risico's voor de rechten en vrijheden van personen in, en nemen zij passende technische of organisatorische maatregelen.[143] Voor online messagingdiensten kan dit bijvoorbeeld inhouden dat zij fors investeren in beveiliging van hun encryptiesysteem om datalekken te voorkomen.

Artikel 7 lid 3 DMA speelt hierop in met betrekking tot de interoperabiliteitsverplichting voor online messagingdiensten: het veiligheidsniveau dat de poortwachter aan zijn eigen gebruikers biedt – met inbegrip van end-to-end encryptie – moet behouden blijven voor alle interoperabele diensten. Bovendien moet de poortwachter volgens lid 4 informatie verschaffen aan de verzoekende dienst over technische details en algemene voorwaarden van interoperabiliteit, waaronder het gewenste veiligheidsniveau. Dat betekent dat een dienst die een interoperabiliteitsverzoek indient bij bijvoorbeeld WhatsApp, moet kunnen verzekeren dat deze dezelfde end-to-end encryptie als WhatsApp kan bieden aan gebruikers, ook als de verzoekende dienst zelf aanvankelijk geen gebruik maakte van deze vorm van versleuteling.

De privacy van gebruikers is overigens het best beschermd als ook de reservekopie van de communicatiegegevens, die in de cloud van de messagingapplicatie en/of smartphoneaanbieder wordt opgeslagen, end-to-end versleuteld is (zie §5.2.3).

---

[140] 'Tegenslag opsporingsdiensten: Apple gaat end-to-endversleuteling in iCloud aanbieden', nos.nl.
[141] Hildenbrand 2021.
[142] 'Backup and Restore Messages', support.signal.org.
[143] Artikel 5(1)(f) jo artikel 32 AVG.

5.2.5 Risico's voor end-to-end encryptie en beveiliging door interoperabiliteit

De interoperabiliteitsverplichting voor online messagingdiensten in artikel 7 DMA kan volgens sommige auteurs veiligheidsrisico's met zich meebrengen voor de end-to-end encryptie en de beveiliging van gegevens in het algemeen.[144] The Verge interviewde verschillende beveiligingsexperts, en een deel van hen stelde dat het erg ingewikkeld en misschien zelfs onmogelijk zal zijn om end-to-end encryptie te behouden tussen interoperabele diensten. Zij wijzen op de technische moeilijkheden die ontstaan wanneer verschillende vormen van encryptie van verschillende diensten samen moeten smelten.[145] De organisatie Matrix, die een open standaard ontwikkelde voor online messaging, stelt hiernaast dat wanneer interoperabele diensten niet dezelfde protocollen gebruiken, de berichten altijd opnieuw moeten worden versleuteld voor dat andere systeem. Dit zorgt ervoor dat de ene dienst erop moet vertrouwen dat de andere dienst de berichten veilig houdt. Dit vergroot volgens Matrix de kans op een aanval op de communicatie, wat de end-to-end encryptie in gevaar brengt.[146] EFF erkent deze gevaren voor encryptie ook, en vindt bovendien dat de DMA poortwachters te weinig tijd geeft om de end-to-end encryptie goed in te richten. Ook wijst EFF erop dat de DMA poortwachters en de Europese Commissie geen middelen geeft om informatie over de mate van encryptie op te vragen bij de verzoekende online messagingdienst.[147]

Maar niet alle experts verwachten dat een interoperabiliteitsverplichting end-to-end encryptie dusdanig onder druk gaat zetten. Volgens Brown kunnen bestaande technische protocollen de basis vormen voor interoperabiliteit en tegelijkertijd veiligheidskenmerken zoals encryptie handhaven.[148] Een interoperabiliteitsverplichting is dus niet per definitie onverenigbaar met end-to-end encryptie, of schadelijk voor de veiligheid en de privacy van gebruikers.[149] Bovendien draagt Matthew Hodgson, medeoprichter van Matrix, verschillende technische oplossingen aan om end-to-end encryptie wel te kunnen handhaven bij interoperabiliteit.[150]

Naast risico's met betrekking tot end-to-end encryptie maken sommige experts zich ook zorgen over beveiliging van de diensten in het algemeen. Een kleine derde partij beschikt bijvoorbeeld niet over dezelfde middelen om zich tegen hacken te beschermen als grote poortwachters,

[144] Brown 2022b; Faife 2022; OECD 2021; Stoltz e.a. 2022.
[145] Faife 2022.
[146] Hodgson 2022a.
[147] Stoltz e.a. 2022.
[148] Brown 2022d.
[149] Brown 2022b.
[150] Hodgson 2022b.

waardoor interoperabiliteit kwetsbaarheden kan creëren. Uiteindelijk is de algehele beveiliging zo sterk als de zwakste schakel.[151] Als deze derde partij bijvoorbeeld interoperabel is met WhatsApp, kunnen door een hack ook de verkeersgegevens van WhatsApp-gebruikers op straat komen te liggen. Hierbij komt dat hoe meer diensten onderling communicatie uitwisselen, hoe meer aanvalspunten er zijn voor hackers om deze (verkeers)gegevens te onderscheppen. Centralisatie is hiervoor een gevaarlijke dynamiek, omdat al deze gegevens zich plotseling op één punt bevinden.[152] Matrix erkent ook dat interoperabiliteit meer misbruik, spam en phishing kan opleveren, maar denkt dit te kunnen lossen met verbeterde anti-misbruik software.[153]

Bovendien is de beveiliging tegen privacy- en veiligheidsrisico's als gevolg van interoperabiliteit erg kostbaar. Dit kan ertoe leiden dat deze kosten tot uiting komen in de toegangsprijzen van de dienst, bijvoorbeeld in de vorm van een advertentiemodel gebaseerd op de analyse van persoonsgegevens.[154]

Al met al heerst er onder experts een technische discussie over de mogelijke risico's van een interoperabiliteitsverplichting voor end-to-end encryptie en beveiliging, welke in dit juridisch onderzoek niet beslecht kan worden. Maar het staat vast dat technici zich zullen moeten inspannen om de beveiliging van communicatie tussen interoperabele diensten te verzekeren, zodat het recht op vertrouwelijkheid van communicatie gewaarborgd blijft en datalekken worden voorkomen.

5.3 Standaardisering

Interoperabiliteit gaat vaak gepaard met standaardisering: de verschillende diensten zullen het eens moeten worden over een gemeenschappelijke standaard (zie §2.4.4). Volgens Brown is de eenvoudigste optie voor standaardisering dat poortwachters beperkte versies van hun eigen API's openbaar maken aan de verzoekende partij, zodat deze hier gebruik van kan maken. Elke poortwachter bepaalt dan dus zelf het veiligheidsniveau, afhankelijk van de gebruikte API's.[155]

5.3.1 Positieve gevolgen van standaardisering voor privacy bij interoperabiliteit

[151] OECD 2021, p. 24; Faife 2022.
[152] Brown 2022a, §6.1.
[153] Hodgson 2022a.
[154] Bourreau e.a. 2022, p. 32-33, 40.
[155] Brown 2022b; Een API is een interface die het mogelijk maakt dat twee systemen met elkaar communiceren.

Standaardisering kan enerzijds positieve gevolgen voor de privacy van gebruikers hebben. In het geval van bijvoorbeeld WhatsApp stimuleert het diensten die interoperabel willen worden om ook end-to-end encryptie in te bouwen, omdat dat nou eenmaal de veiligheidseisen van WhatsApp zijn. Standaardisering zorgt dus ook mogelijk voor een breder gebruik van versleuteling van communicatie in het algemeen, wat bijdraagt aan het recht op vertrouwelijkheid van communicatie en de eerdergenoemde beveiligingseisen in de AVG.

Bovendien is de noodzaak tot standaardisering een kans voor de online messagingmarkt om het privacyvriendelijkste end-to-end ontwerp te kiezen en dit op de gehele markt toe te passen.[156] De Internet Engineering Task Force investeert op dit moment in Messaging Layer Security (MLS), een standaard protocol voor versleutelde communicatie. Volgens experts lijkt MLS in de toekomst in staat om interoperabiliteit tussen online messagingdiensten mogelijk te maken, en tegelijkertijd een hoog veiligheidsniveau van end-to-end encryptie te behouden. Een andere mogelijke kanshebber is het open source protocol van Matrix.[157] De toepassing van een van deze twee protocollen op de belangrijkste online messagingdiensten zou wederom bijdragen aan de vertrouwelijkheid en beveiliging van communicatie.

5.3.2 Negatieve gevolgen van standaardisering voor privacy bij interoperabiliteit

Standaardisering kan volgens sommigen echter ook negatieve consequenties hebben voor beveiliging van communicatie. Volgens artikel 7 lid 1 DMA moeten poortwachters de 'nodige technische interfaces' beschikbaar maken aan verzoekende partijen om de interoperabiliteit mogelijk te maken. Wanneer van de poortwachter verwacht wordt dat deze interfaces stabiel worden aangeboden, kan dit betekenen dat het voor poortwachters lastiger wordt om bijwerkingen of wijzigingen hierin door te voeren. Dit kan negatieve gevolgen hebben voor de beveiliging.[158] Denk aan een innovatieve wijziging in de end-to-end encryptie die niet wordt doorgevoerd omdat de poortwachter dan bang is niet meer te voldoen aan de vereisten in artikel 7 DMA, namelijk het op een toegankelijke manier interoperabiliteit mogelijk maken. Bovendien betekent standaardisering dat de verzoekende partij zelf ook minder makkelijk beveiligingsupdates kan doorvoeren. Moxie Marlinspike, medeoprichter van Signal, heeft

[156] Brown 2022a, §6.1.
[157] Gulati-Gilbert & Knodel 2022; Brown 2022a, §6.1; Brown 2022c.
[158] Cyphers & Doctorow 2021, p. 29.

moeite met dit ‘onaanvaardbaar onvermogen’ om zich aan te passen wanneer Signal interoperabel zou worden met een poortwachtende dienst.[159]

Zoals besproken in §2.4.4 kan standaardisering daarmee mogelijk leiden tot stagnatie van innovatie.[160] Door bovenstaande problematiek bestaat het risico dat standaardisering van end-to-end encryptie in de online messagingmarkt leidt tot minder innovatie op het gebied van communicatiebeveiliging en daarmee de privacy van gebruikers.

[159] Marlinspike 2016.
[160] Brown 2020, p. 25; Crémer 2019, p. 85.

Hoofdstuk 6. Aanbevelingen aan Europese Commissie voor richtsnoeren ex artikel 47 DMA

6.1 Inleiding

Uit de hoofdstukken 3 t/m 5 blijkt dat een interoperabiliteitsverplichting het recht op privacy van gebruikers van online messagingdiensten op verschillende manieren onder druk kan zetten. Hierdoor bestaat het risico dat poortwachters de privacybescherming van gebruikers zullen aangrijpen als reden om niet aan de verplichting te hoeven voldoen, bijvoorbeeld in de vorm van een beroep op artikel 7 lid 9 DMA. Hier ligt een belangrijke taak voor de Commissie. In richtsnoeren kan zij met scherpe aanwijzingen en verduidelijkingen aantonen dat met de juiste maatregelen de privacy van gebruikers wel degelijk gewaarborgd kan worden. In dit hoofdstuk doe ik aanbevelingen aan de Commissie voor het opstellen van richtsnoeren ex artikel 47.

6.2 Informatieverschaffing door verzoekende partij

Volgens artikel 7 lid 4 DMA moet de poortwachter allerlei informatie verschaffen aan de verzoekende partij, namelijk de technische details en algemene voorwaarden voor interoperabiliteit, waaronder de nodige informatie over het veiligheidsniveau en end-to-end encryptie. Verzoekende diensten hebben echter niet een dusdanige verplichting. Voor een betere bescherming van het recht op privacy van gebruikers is het essentieel dat ook verzoekende diensten voldoende informatie verschaffen aan de poortwachter. In de verzoekfase worden namelijk de privacyrisico's ingeschat en kan een poortwachter mogelijk maatregelen treffen ex artikel 7 lid 9, of uitstel vragen ex artikel 7 lid 6 DMA.

Met betrekking tot end-to-end encryptie zullen verzoekende diensten naar verwachting gebruikmaken van het protocol van de poortwachter zelf of een nieuwe gemeenschappelijke standaard, dus hierover is waarschijnlijk geen informatieverstrekking nodig. Informatie over de beveiliging van een verzoekende dienst is daarentegen wel essentieel voor de poortwachter om te weten of het veiligheidsniveau behouden blijft, en hoe kwetsbaar een verzoekende dienst is voor bijvoorbeeld hacken en datalekken. Bovendien is het van belang dat de poortwachter voldoende informatie heeft over het privacybeleid van de verzoekende partij, zodat het haar gebruikers goed kan informeren over de gevolgen van het verzenden van communicatie naar de andere dienst. Met name van belang is welke verkeersgegevens de verzoekende partij verwerkt en hoe lang deze bewaard worden.

Het verdient aanbeveling dat de Commissie in de richtsnoeren ex artikel 47 DMA poortwachters aanraadt zoveel mogelijk informatie over beveiliging en (verkeers)gegevensverwerking op te vragen bij de verzoekende partij, om de privacy van gebruikers zo goed mogelijk te beschermen.

6.3 Verkeersgegevens nodig voor 'effectieve' interoperabiliteit

Verder kan de Commissie in richtsnoeren verduidelijken welke verkeersgegevens precies nodig zijn om een 'effectieve interoperabiliteit' te waarborgen zoals vereist in artikel 7 lid 8 DMA, en hoe lang deze gegevens bewaard moeten worden. Dit draagt bij aan de beginselen van dataminimalisatie en doelbinding uit de AVG. Het is nu namelijk onduidelijk wanneer het doel van interoperabiliteit precies bereikt is: welke gegevens zijn hiervoor essentieel, en kunnen zij verwijderd worden nadat de communicatieoverdracht heeft plaatsgevonden?

De Commissie zou in haar richtsnoeren een voorstel kunnen doen voor een maximale bewaartermijn die moet gelden voor verkeersgegevens die verwerkt worden ten behoeve van interoperabiliteit. Zij zou hiertoe advies kunnen inwinnen bij de EDPB en technische experts. Deze adviesbewaartermijn kan dan door interoperabele partijen overgenomen worden in hun privacyvoorwaarden.

6.4 Just-in-time informatieverschaffing

In haar richtsnoeren kan de Commissie online messagingdiensten bovendien adviseren om een waarschuwingspop-up in te bouwen wanneer een gebruiker naar een gebruiker op een andere, interoperabele dienst wil communiceren (zie §4.4.3). Deze *just-in-time* informatieverschaffing sluit zo goed mogelijk aan bij de vereisten in de AVG en draagt bovendien bij aan het zelfbeschikkingsrecht over communicatie. Tegelijkertijd moet aan interoperabele partijen wel de ruimte worden gelaten om zelf met creatieve oplossingen te komen.

Het risico blijft bestaan dat poortwachters deze waarschuwingspop-up zullen misbruiken om gebruikers af te schrikken voor communicatie met een andere dienst. De Commissie kan dit gevaar in haar richtsnoeren in ieder geval aan het licht brengen.

6.5 Veilige standaard voor end-to-end encryptie

Over end-to-end encryptie en beveiliging wordt voornamelijk een technische discussie gevoerd onder experts. Het recht op vertrouwelijkheid van communicatie en

persoonsgegevensbescherming is het best gebaat bij een goed functionerende end-to-end encryptie en een solide beveiliging. Mogelijk kunnen de Europese normalisatie-instellingen, zoals genoemd in overweging 96 DMA, adviseren over een veilige standaard die over de gehele markt kan worden toegepast, zoals het aankomende MSL of het open protocol van Matrix. De Commissie zou het gebruik van deze gemeenschappelijke standaard dan in richtsnoeren ex artikel 47 DMA kunnen aanraden aan poortwachters en verzoekende partijen.

Politiek ligt dit echter gevoelig. Er veel druk vanuit overheden om end-to-end encryptie in messaging te beperken. Toch zou het aanbevelen van deze gemeenschappelijke standaard – kijkend naar de in dit onderzoek geschetste risico's – een belangrijke stap kunnen zijn in de bescherming van het recht op privacy van gebruikers.

6.6 Privacywaarborgen blijven verbeteren na interoperabiliteit

Door standaardisering bestaat het risico dat wijzigingen in de technische interfaces van poortwachters minder gemakkelijk worden doorgevoerd. Dit kan beveiligingsproblemen en stagnatie van innovatie op privacygebied in de hand werken. De Commissie kan in haar richtsnoeren verduidelijken dat het 'behouden' van een bepaald veiligheidsniveau ex artikel 7 lid 3 DMA inhoudt dat de partijen ook na interoperabiliteit nieuwe risico's voor de privacy van gebruikers blijven inschatten en hierop acteren. Hiertoe kan de Commissie online messagingdiensten aanbevelen om bij twijfel advies in te winnen bij de Europese normalisatie-instellingen, zoals genoemd in overweging 96 DMA.

Hoofdstuk 7. Conclusie

De interoperabiliteitsverplichting voor poortwachtende online messagingdiensten in artikel 7 DMA heeft een mededingingsrechtelijk doeleinde, namelijk het creëren van een eerlijkere markt en het verminderen van de macht van dominante platformen die profiteren van sterke netwerkeffecten. Deze verplichting heeft echter ook consequenties voor de privacy van gebruikers. In dit onderzoek stond de volgende onderzoeksvraag centraal:

Hoe kan bij de implementatie van de interoperabiliteitsverplichting voor online messagingdiensten in artikel 7 DMA de grootst mogelijke bescherming worden geboden aan het recht op privacy van gebruikers, specifiek het recht op vertrouwelijkheid van communicatie en persoonsgegevensbescherming?

Enerzijds kan de interoperabiliteitsverplichting bijdragen aan sterkere waarborgen voor het recht op privacy van gebruikers. Interoperabiliteit vermindert de sterke netwerkeffecten en *lock-in* waarvan poortwachters profiteren, waardoor er mogelijk meer concurrentie ontstaat en gebruikers een daadwerkelijke keuze hebben voor een alternatieve online messagingdienst die betere privacybescherming biedt. Bovendien kan interoperabiliteit ervoor zorgen dat online messagingdiensten een commercieel belang hebben om de beste privacybescherming te bieden, wat kan leiden tot meer innovatie op privacygebied. Ook kan interoperabiliteit leiden tot een grootschaliger gebruik van end-to-end encryptie binnen de online messagingmarkt en biedt het de kans aan de markt om het privacyvriendelijkste end-to-end ontwerp als standaard te kiezen.

Anderzijds zorgt de interoperabiliteitsverplichting voor een bredere uitwisseling van communicatiegegevens, waardoor de vermeend betere privacybescherming van een alternatieve, interoperabele dienst onder druk komt te staan, met name op het gebied van dataminimalisatie en doelbinding. Naar verwachting zal toestemming als grondslag worden gebruikt voor deze aanvullende persoonsgegevensverwerking in het kader van interoperabiliteit. Hierbij moet rekening worden gehouden met het risico op *pop-up fatigue* en een in wezen onvrijwillige en ongeïnformeerde toestemming van gebruikers.

Over de gevolgen van interoperabiliteit voor end-to-end encryptie en beveiliging wordt in de literatuur gesteggeld. Sommige experts menen dat interoperabiliteit en betrouwbare end-to-end encryptie en beveiliging niet samen kunnen gaan, anderen wijzen op technische oplossingen

die dit wel mogelijk moeten maken. Standaardisering in de online messagingmarkt zorgt er bovendien mogelijk voor dat online messagingdiensten minder makkelijk wijzigingen in hun protocollen kunnen doorvoeren, wat uiteindelijk ook kan leiden tot stagnatie van innovatie op het gebied van privacybescherming voor gebruikers.

De uitkomst van deze wirwar aan voors en tegens zal sterk afhangen van technische (on)mogelijkheden en het gedrag van gebruikers en de markt. Dit bepaalt uiteindelijk of eerlijke mededinging bijvoorbeeld zal zorgen voor meer innovatie op privacygebied, of juist tot standaardisering die deze innovatie remt. Consumentengedrag zal bepalen of diensten zullen gaan concurreren op privacy, of toch op prijs. De techniek zal bepalen of end-to-end encryptie en beveiliging overeind blijven. Bovendien kan het voor privacyrechtelijke alternatieven vanuit reputatieoverwegingen onaantrekkelijk zijn om interoperabel te worden met een poortwachter. De gevolgen voor de privacy van gebruikers zijn van dit alles afhankelijk.

De Commissie kan in richtsnoeren ex artikel 47 DMA echter handvatten bieden om de privacyrisico's zoveel mogelijk in te perken. Bovendien kunnen poortwachters dan minder makkelijk een beroep doen op deze risico's om de interoperabiliteitsverplichting vleugellam te maken. Allereerst kan de Commissie poortwachters in haar richtsnoeren adviseren om voldoende relevante informatie op te vragen bij de verzoekende partij over privacybescherming. Daarnaast kan de Commissie verduidelijken wat zij precies verstaat onder gegevens die noodzakelijk zijn om een effectieve interoperabiliteit te waarborgen. Verder kan zij poortwachters adviseren om gebruikers die communiceren via interoperabele diensten *just-in-time* informatie te verschaffen over de gevolgen hiervan. Belangrijk is wel dat deze informatie objectief is. Ook kan de Commissie poortwachters aanraden om een bepaalde gemeenschappelijke standaard te gebruiken voor end-to-end encryptie en beveiliging van de dienst. Tot slot kan de Commissie in richtsnoeren verduidelijken dat het veiligheidsniveau ook na interoperabiliteit gewaarborgd moet worden, bijvoorbeeld door wijzigingen door te voeren of te innoveren.

Deze inspanning van de Commissie middels richtsnoeren is naar mijn mening cruciaal om de interoperabiliteitsverplichting van artikel 7 DMA vleugels te geven, en tegelijkertijd het recht op privacy van gebruikers te waarborgen.

Appendix – Relevante DMA-bepalingen

N.B. Een aantal kernwoorden die in het bijzonder relevant zijn voor dit onderzoek zijn dikgedrukt weergegeven.

Overweging 64 DMA

Door het gebrek aan interoperabiliteit kunnen poortwachters die nummeronafhankelijke interpersoonlijke communicatiediensten aanbieden, profiteren van sterke netwerkeffecten, wat de betwistbaarheid afzwakt. Bovendien bieden poortwachters, ongeacht of het gaat om "multihome"-eindgebruikers, vaak nummeronafhankelijke interpersoonlijke communicatiediensten aan als onderdeel van hun platformecosysteem, waardoor de toetredingsdrempels voor andere aanbieders van dergelijke diensten nog hoger worden en de kosten voor eindgebruikers om over te stappen, stijgen. Onverminderd Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad en met name de voorwaarden en procedures van artikel 61, moeten poortwachters daarom, kosteloos en op verzoek, interoperabiliteit met bepaalde basisfuncties van de nummeronafhankelijke interpersoonlijke communicatiediensten die zij aan hun eindgebruikers verlenen, waarborgen aan derde aanbieders van dergelijke diensten.

Poortwachters moeten zorgen voor interoperabiliteit voor derde aanbieders die hun nummeronafhankelijke interpersoonlijke communicatiediensten verlenen of voornemens zijn te verlenen aan eindgebruikers en zakelijke gebruikers in de Unie. Om de praktische uitvoering van die interoperabiliteit te vergemakkelijken, moet de betrokken poortwachter worden verplicht een referentieofferte te publiceren met de technische details en algemene voorwaarden inzake interoperabiliteit met zijn nummeronafhankelijke interpersoonlijke communicatiediensten. De Commissie moet indien nodig het Orgaan van Europese regelgevende instanties voor elektronische communicatie kunnen raadplegen om te bepalen of de technische details en de algemene voorwaarden die zijn bekendgemaakt in de referentieofferte die de poortwachter voornemens is toe te passen of heeft toegepast, de naleving van die verplichting waarborgen.

In alle gevallen moeten de poortwachter en de verzoekende aanbieder ervoor zorgen dat de interoperabiliteit een hoog niveau van **veiligheid en gegevensbescherming** niet in de weg staat,

overeenkomstig hun verplichtingen uit hoofde van deze verordening en het toepasselijke Unierecht, met name Verordening (EU) 2016/679 en Richtlijn 2002/58/EG. De verplichting met betrekking tot interoperabiliteit mag geen afbreuk doen aan de informatie en keuzes die uit hoofde van deze verordening en andere wetgeving van de Unie, met name Verordening (EU) 2016/679, beschikbaar moeten worden gesteld aan eindgebruikers van de nummeronafhankelijke interpersoonlijke communicatiediensten van de poortwachter en de verzoekende aanbieder.

Artikel 7 DMA

1. Een poortwachter die nummeronafhankelijke interpersoonlijke communicatiediensten aanbiedt welke op grond van artikel 3, lid 9, zijn opgenomen in het aanwijzingsbesluit, zorgt ervoor dat de basisfuncties van zijn nummeronafhankelijke interpersoonlijke communicatiediensten interoperabel zijn met de nummeronafhankelijke interpersoonlijke communicatiediensten van een andere aanbieder die dergelijke diensten in de Unie verleent of voornemens is dat te doen. Daartoe maakt de poortwachter de nodige technische interfaces of soortgelijke oplossingen met het oog op interoperabiliteit op verzoek en kosteloos beschikbaar.

2. De poortwachter maakt ten minste de volgende in lid 1 bedoelde basisfuncties interoperabel wanneer hij die functies zelf aan zijn eindgebruikers aanbiedt:

a) na de opname in het aanwijzingsbesluit op grond van artikel 3, lid 9:

i) eind-tot-eindtekstberichten tussen twee afzonderlijke eindgebruikers;

ii) uitwisseling van afbeeldingen, spraakberichten, video's en andere bijgevoegde bestanden bij eind-tot-eindcommunicatie tussen twee afzonderlijke eindgebruikers;

b) binnen twee jaar na de aanwijzing:

i) eind-tot-eindtekstberichten tussen groepen afzonderlijke eindgebruikers;

ii) uitwisseling van afbeeldingen, spraakberichten, video's en andere bijgevoegde bestanden bij eind-tot-eindcommunicatie tussen een groepschat en een afzonderlijke eindgebruiker;

c) binnen vier jaar na de aanwijzing:

i) eind-tot-eindspraakgesprekken tussen twee afzonderlijke eindgebruikers;

ii) eind-tot-eindvideogesprekken tussen twee afzonderlijke eindgebruikers;

iii) eind-tot-eindspraakgesprekken tussen een groepschat en een afzonderlijke eindgebruiker;

iv) eind-tot-eindvideogesprekken tussen een groepschat en een afzonderlijke eindgebruiker.

3. Het **veiligheidsniveau**, met in voorkomend geval **eind-tot-eindversleuteling**, dat de poortwachter zijn eindgebruikers biedt, is hetzelfde voor alle interoperabele diensten.

4. De poortwachter publiceert een referentieofferte met daarin de technische details en algemene voorwaarden voor interoperabiliteit met zijn nummeronafhankelijke interpersoonlijke communicatiediensten, waaronder de nodige informatie over het veiligheidsniveau en de eind-tot-eindversleuteling. De poortwachter publiceert die referentieofferte binnen de in artikel 3, lid 10, vastgestelde termijn en actualiseert die wanneer nodig.

5. Na publicatie van de referentieofferte op grond van lid 4, kan elke aanbieder van nummeronafhankelijke interpersoonlijke communicatiediensten die die diensten in de Unie verleent of voornemens is dat te doen om interoperabiliteit verzoeken met de door de poortwachter aangeboden nummeronafhankelijke interpersoonlijke communicatiediensten. Dat verzoek kan alle of een deel van de in lid 2 bedoelde basisfuncties betreffen. De poortwachter geeft binnen drie maanden na ontvangst van een redelijk verzoek tot interoperabiliteit daaraan gehoor door de verzochte basisfuncties operationeel te maken.

6. Op gemotiveerd verzoek van de poortwachter kan de Commissie bij wijze van uitzondering de nalevingstermijnen uit hoofde van lid 2 of lid 5 verlengen, mits de poortwachter aantoont dat dat noodzakelijk is om effectieve interoperabiliteit te waarborgen en om het noodzakelijke veiligheidsniveau, in voorkomend geval met eind-tot-eindversleuteling, te handhaven.

7. Het blijft de eindgebruikers van de nummeronafhankelijke interpersoonlijke communicatiediensten van de poortwachter en van de verzoekende aanbieder van nummeronafhankelijke interpersoonlijke communicatiediensten vrijstaan te beslissen of zij al dan niet gebruikmaken van de interoperabele basisfuncties die de poortwachter op grond van lid 1 kan aanbieden.

8. De poortwachter verzamelt van eindgebruikers alleen de **persoonsgegevens die strikt noodzakelijk zijn voor effectieve interoperabiliteit** en wisselt alleen die gegevens uit met de aanbieder van nummeronafhankelijke interpersoonlijke communicatiediensten die om interoperabiliteit verzoekt. Bij het verzamelen en uitwisselen van de persoonsgegevens van eindgebruikers moeten Verordening (EU) 2016/679 en Richtlijn 2002/58/EG volledig in acht worden genomen.

9. Het wordt de poortwachter niet belet maatregelen — voor zover die strikt noodzakelijk en evenredig zijn — te treffen om ervoor te zorgen dat derde aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten die om interoperabiliteit verzoeken de **integriteit, veiligheid en privacy** van zijn diensten niet in het gedrang brengen, maar hij is wel gehouden dat naar behoren te motiveren.

Literatuurlijst

N.B. Voor de bronvermelding is in dit onderzoek gebruik gemaakt van de *Leidraad voor juridische auteurs*, editie 2022.

Boeken, rapporten, officiële publicaties, artikelen en webpagina's

Afonin 2021
O. Afonin, 'Apple Scraps End-to-End Encryption of iCloud Backups', blog.elcomsoft.com, 6 januari 2021.

Alexander 2021
L.M. Alexander, *Privacy and Antitrust at the Crossroads of Big Tech*, Washington: American Antitrust Institute 2021.

Arnbak 2015
A.M. Arnbak, *Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives*, Amsterdam: IViR 2015.

Arnold e.a. 2020
R. Arnold, A. Schneider, J. Lennartz, 'Interoperability of interpersonal communications services – A consumer perspective', *Telecommunications Policy* (44) April 2020, afl. 3.

Arnold e.a. 2017
R. Arnold & A. Schneider, *An App for Every Step: A psychological perspective on interoperability of Mobile Messenger Apps, 28th European Regional Conference of the International Telecommunications Society (ITS): "Competition and Regulation in the Information Age", Passau, Germany, 30th July - 2nd August, 2017*, Caldary: International Telecommunications Society 2017.

Arnold e.a. 2016

R. Arnold, A. Schneider, C. Hildebrandt, *All communications services are not created equal – substitution of OTT communications services for ECS from a consumer perspective,* TPRC44 Paper 2016.

ARTICLE 19 2020

ARTICLE 19, *How The Internet Really Works*, San Francisco: No Starch Press 2020.

Bagloni e.a. 2016

F. Bagloni e.a*., Internet Science*: *Third International Conference, INSCI 2016, Florence, Italy, September 12-14, 2016, Proceedings*, Cham: Springer International Publishing 2016.

Barczentewicz 2022

M. Barczentewicz, *Privacy and Security Implications of Regulation of Digital Services in the EU and in the US*, Stanford: TTLF Working Papers 2022.

BEREC 2021

BEREC, *BEREC Report on the interplay between the EECC and the EC's proposal for a Digital Markets Act concerning number-independent interpersonal communication services*, BoR (21) 85, Riga: BEREC 2021.

Bouma 2019

R. Bouma, 'Minister Grapperhaus wil toegang tot chat- en berichtendiensten', nos.nl, 3 november 2019.

Bourreau e.a. 2022

M. Bourreau, J. Krämer & M. Buiten, *Interoperability in Digital Markets*, Brussel: Centre on Regulation in Europe 2022.

Bravo-Lillo e.a. 2014

C. Bravo-Lillo, L. Cranor, S. Komanduri, S. Schechter & M. Sleeper, 'Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It', in: *10th Symposium On Usable Privacy and Security (SOUPS)*, Berkeley: USENIX Association 2014.

Brown 2022a

I. Brown, *Private messaging Interoperability in the EU Digital Markets Act*, Redwood City: Omidyar Network 2022 [confidential draft].

Brown 2022b

I. Brown, 'Key points on DMA interoperability and encryption', ianbrown.tech, 1 april 2022.

Brown 2022c

I. Brown, 'End-to-end encrypted group chats and interoperability', interoperability.news, 18 maart 2022.

Brown 2022d

I. Brown, 'Interoperability in one minute', ianbrown.tech, 24 februari 2022.

Brown 2020

I. Brown, *Interoperability as a tool for competition regulation*, Brussel: OpenForum Academy 2020.

Brown & Korff 2022

I. Brown & D. Korff, 'Data protection and digital competition - European Union', ianbrown.tech, 6 mei 2022.

Busch e.a. 2021

C. Busch, I. Graef, J. Hofmann and A. Gawer, *Uncovering blindspots in the policy debate on platform power*, Brussel: Europese Commissie 2021.

Council of Europe 2021

Council of Europe, *Guide on Article 8 of the European Convention of Human Rights,* Straatsburg: Raad van Europa 2021.

Council of Europe e.a. 2019

Council of Europe, European Court of Human Rights, European Data Protection Supervisor and European Union Agency for Fundamental Rights, *Handbook on European data protection law: 2018 edition*, Straatsburg: Publications Office 2019.

Crémer e.a. 2019

J. Crémer, Y.-A. De Montjoye, & H, Schweitzer, *Competition policy for the digital era*, Brussel: Europese Commissie 2019.

Cyphers & Doctorow 2021

B. Cyphers & C. Doctorow, 'Privacy Without Monopoly: Data Protection and Interoperability', eff.org, 12 februari 2021.

Cyphers & Doctorow 2020

B. Cyphers & C. Doctorow, 'A Legislative Path to an Interoperable Internet', eff.org, 28 juli 2020.

Dallal 2022

A. Dallal, 'Most Popular Messaging Apps Around the Globe (Updated: May 2022)', similarweb.com, 28 juni 2022.

Dixon 2022

S. Dixon, 'Most popular global mobile messenger apps as 2022', statista.com, 27 juli 2022.

EDPB 2020

European Data Protection Board, *Statement on the data protection impact of the interoperability of contact tracing apps*, Brussel: EDPB 2020.

Endeley 2018

R.E. Endeley, 'End-to-End Encryption in Messaging Services and National Security – Case of WhatsApp Messenger', *Journal of Information Security* (9) 23 januari 2018, afl. 1, p. 95-99.

Faife 2022

C. Faife, 'Security experts say new EU rules will damage WhatsApp encryption', theverge.com, 28 mei 2022.

FTC 2013

Federal Trade Commission, *Mobile Privacy Disclosures: Building Trust Through Transparency: A Federal Trade Commission Staff Report*, Washington: Federal Trade Commission 2013.

Furman e.a. 2019

J. Furman, D. Coyle, A. Fletcher, P. Marsden & D. McAuley, *Unlocking digital competition: Report of the digital competition expert panel*, Londen: HM Treasury 2019.

Geradin 2022

D. Geradin, 'The leaked "final" version of the Digital Markets Act: A summary in ten points', theplatformlaw.blog, 19 april 2022.

González e.a. 2020

E.G. González, P. De Hert, V. Papakonstantinou, *The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads?*, Brussel: Brussels Privacy Hub 2020.

Griggio e.a. 2022

C.F. Griggio, M. Nouwens and C. Nylandsted Klokmose, 'Caught in the Network: The Impact of WhatsApp's 2021 Privacy Policy Update on Users' Messaging App Ecosystems', *CHI Conference on Human Factors in Computing Systems* 2022, Association for Computing Machinery, New York, NY, USA, Article 104, p. 1–23.

Gulati-Gilbert & Knodel 2022

S. Gulati-Gilbert & M. Knodel, 'Preserving the Open Internet Through Interoperability', cdt.org, 21 juli 2022.

Hijnk & Wassens 2022

M. Hijnk & R. Wassens, 'WhatsApp dreigde uit Nederland te vertrekken om aftapplicht', nrc.nl, 3 juni 2022.

Hildenbrand 2021

J. Hildenbrand, ‘How Google's backup encryption works: The good, the bad, and the ugly’, androidcentral.com, 4 mei 2021.

Hodgson 2022a

M. Hodgson, ‘How do you implement interoperability in a DMA world?’, matrix.org, 29 maart 2022.

Hodgson 2022b

M. Hodgson, ‘Interoperability without sacrificing privacy: Matrix and the DMA’, matrix.org, 25 maart 2022.

Kranenborg, in: *The EU Charter of Fundamental Rights: A Commentary* 2014

H. Kranenborg, ‘Article 8’, in: S. Peers et al, *The EU Charter of Fundamental Rights: A Commentary*, Oxford: Beck/Hart/Nomos 2014.

Larouche & De Streel 2021

Pierre Larouche and Alexandre de Streel,‘The European Digital Markets Act: A Revolution Grounded on Traditions’, *Journal of European Competition Law & Practice* (12) 27 augustus 2021, afl. 7, p. 542-560.

Marlinspike 2016

M. Marlinspike, ‘Reflections: The ecosystem is moving’, signal.org, 10 mei 2016.

Marsden & Podszun 2020

P. Marsden & R. Podszun, *Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement*, Berlijn: Konrad-Adenauer-Stiftung 2020.

Moore & Tambini 2018

M. Moore & D. Tambini (eds.), *Digital Dominance: The Power of Google, Amazon, Facebook and Apple,* Oxford: Oxford University Press 2018.

Newton 2021

C. Newton, ‘The battle inside Signal’, theverge.com, 26 januari 2021.

OECD 2021

Organisation for Economic Co-operation and Development, *Data portability, interoperability and digital platform competition*, Parijs: OECD Competition Committee Discussion Paper 2021.

O'Flaherty 2021

K. O'Flaherty, 'Is it time to leave WhatsApp – and is Signal the answer?', theguardian.com, 24 januari 2021.

Patel 2022

N. Patel, 'Why Signal won't compromise on encryption, with president Meredith Whittaker', theverge.com, 19 oktober 2022.

Scott Morton e.a. 2021

F.M. Scott Morton, G.S. Crawford, J. Crémer, D. Dinielli, A. Fletcher, P. Heidhues, M. Schnitzer & K. Seim, *Equitable Interoperability: The 'Super Tool' of Digital Platform Governance*, Yale: Tobin Center for Economic Policy 2021.

Scott Morton e.a. 2019

F.M. Scott Morton, P. Bouvier, A. Ezrachi, B. Jullien, R. Katz, G. Kimmelman, A.D. Melamed, J. Morgenstern, *Committee for the Study of Digital Platforms Market Structure and Antitrust Subcommittee Report*, Chicago: Stigler Centre 2019.

Steenbruggen 2009

W.A.M. Steenbruggen, *Publieke dimensies van privé-communicatie: een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk*, Amsterdam: Otto Cramwinckel Uitgever 2009.

Stoltz e.a. 2022

M. Stoltz, A. Crocker & C. Schmon, 'The EU Digital Markets Act's Interoperability Rule Addresses An Important Need, But Raises Difficult Security Problems for Encrypted Messaging', eff.org, 2 mei 2022.

Tarkowski e.a. 2022

A. Tarkowski, S. Bloemen, P. Keller & T. De Groot, *Generative Interoperability Building Online Public And Civic Spaces*, Amsterdam: Common Network and Open Future 2022.

Van Dijck e.a. 2019

J. van Dijck, D. Nieborg and T. Poell, 'Reframing platform power', *Internet Policy Review* (8) 2019, afl. 2.

Van Dijk 2022

W. van Dijk, 'Veel kritiek op plannen van Brussel om bedrijven te verplichten kinderporno op te sporen', nrc.nl, 11 mei 2022.

Van Hoboken & Zuiderveen Borgesius 2015

J. van Hoboken & F.J. Zuiderveen Borgesius, 'Scoping Electronic Communication Privacy Rules: Data, Services and Values.', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (6) 2015, afl. 3, p. 198-210.

Vegelien 2019

S. Vegelien, 'Telegram heeft meer dan 500 miljoen gebruikers na recente toestroom', tweakers.net, 13 januari 2021.

Vermeulen 2021

M. Vermeulen, 'Persoonlijk klantcontact: er komt een revolutie aan', frankwatching.com, 24 juni 2021.

Warofka 2022

A. Warofka, 'Independent Assessment: Expanding End-to-End Encryption Protects Fundamental Human Rights', about.fb.com, 4 april 2022.

Whittaker 2022

M. Whittaker, 'Signal's also end to end encrypted!', twitter.com, 19 oktober 2022.

Windwehr & Schmon 2020

S. Windwehr and C. Schmon, 'Our EU Policy Principles: Interoperability', eff.org, 18 juni 2020.

Winokur Munk 2022

C. Winokur Munk, 'Why Mark Zuckerberg is talking so much about Meta's Whatsapp for business', cnbc.com, 7 augustus 2022.

Zuiderveen Borgesius & Steenbruggen 2019

F.J. Zuiderveen Borgesius & W.A.M. Steenbruggen, 'The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust.', *Theoretical inquiries in law* (19) 2019, afl. 2, p. 291-322.

Zwenne 2018

G.J. Zwenne, 'Commentaar op hoofdstuk 11 Tw', in: G.J. Zwenne & P.C. Knol, *Tekst & Commentaar Privacy- en telecommunicatierecht*, Deventer: Wolters Kluwer 2018.

<u>Jurisprudentie</u>

Europese Hof van Justitie

HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*)

HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2/Watson*)

HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*Prokuratuur)*

Europees Hof voor de Rechten van de Mens

EHRM 5 september 2017, ECLI:CE:ECHR:2017:0905JUD006149608 (*Bărbulescu v. Romania*)

EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch*)

Regelgeving

Raad van Europa

Europees Verdrag voor de Rechten van de Mens

Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, Rome, 4 april 1950.

Europese Unie

Algemene Verordening Gegevensbescherming

Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (*PbEU* 2016, L 119/1).

Digital Markets Act

Verordening 2022/1925 van het Europees Parlement en de Raad van 14 september 2022 over betwistbare en eerlijke markten in de digitale sector, en tot wijziging van Richtlijnen 2019/1937 en 2020/1828 (digitalemarktenverordening) (*PbEU* 2022, L 265/1).

ePrivacy Richtlijn

Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (*PbEU* 2002, L 201/37).

ePrivacy Verordening

Voorstel voor een Verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie). Brussel, 10.01.2017; COM(2017) 10 final; 2017/0003 (COD).

Europees wetboek voor elektronische communicatie

Richtlijn 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (europees wetboek voor elektronische communicatie) (*PbEU*, L 321/36).

Handvest van de Grondrechten van de Europese Unie

Handvesten van de Grondrechten van de Europese Unie, Straatsburg, 18 december 2000, 2000/C 364/01.

Impact Assessment DMA

Commission Staff Working Document Impact Assessment Report, Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act). Brussel, 15.12.2020; SWD (2020) 363 final.

Platform-to-Business Verordening

Verordening 2019/1150 van het Europees Parlement en de Raad van 20 juni 2019 ter bevordering van billijkheid en transparantie voor zakelijke gebruikers van onlinetussenhandelsdiensten (platform-to-business verordening) (*PbEU*, L 186/57).