# De Europese Unie als een constitutionele waakhond van privacy en gegevensbescherming op internet: het verhaal van artikel 16 VWEU ("The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU")

## KORTE SAMENVATTING


Er bestaat de perceptie dat overheden controle verliezen over maatschappelijke ontwikkelingen, als gevolg van globalisering en technologische fenomenen. Deze verschijnselen verhinderen een effectieve bescherming van fundamentele waarden in democratische samenlevingen. Voorbeelden van problemen zijn de extensieve toegang van de Amerikaanse NSA tot persoonsgegevens van Europeanen, zoals naar voren kwam in de onthullingen van Edward Snowden, en de moeite die het kost om in een big data omgeving te zorgen dat de grote internetbedrijven goede privacy-voorwaarden hanteren, waarbij de burger nog enige controle heeft over wat er met zijn gegevens gebeurt.

Deze studie gaat over privacy en gegevensbescherming als fundamentele waarden in de democratische rechtsstaat. De EU Verdragen hebben de Europese Unie een breed geformuleerde opdracht gegeven om deze grondrechten effectief te beschermen, door middel van rechterlijk toezicht, wetgeving en toezicht door onafhankelijke autoriteiten. Het mandaat is nu op constitutioneel niveau vastgelegd en geeft de Unie het vermogen om op te treden als een constitutionele waakhond van privacy en gegevensbescherming.

Meer precies, Artikel 16 van het EU Werkingsverdrag (VWEU), gelezen in samenhang met de artikelen 7 en 8 van het Grondrechtenhandvest, legt de taken vast van de Unie op dit terrein. Artikel 16 (1) VWEU en de artikelen 7 en 8 Handvest specificeren het recht dat de Unie moet garanderen, uiteindelijk onder toezicht van het Europees Hof van Justitie, artikel 16 (2) VWEU geeft de wetgever de opdracht regels te stellen en tot slot moet het toezicht door de onafhankelijke autoriteiten worden gegarandeerd, een vereiste van artikel 16 (2) VWEU en artikel 8 (3) Handvest.

Artikel 16 VWEU geeft de Unie een specifiek mandaat om bescherming te verzekeren, in aanvulling op de algemene verplichting voor de Unie - en voor de nationale overheden wanneer zij handelen binnen de reikwijdte van het Europees recht - om de rechten in het Handvest te respecteren. Artikel 16 VWEU bepaalt *dat* de Unie moet optreden ter bescherming van de grondrechten van privacy en gegevensbescherming.

De opdracht van artikel 16 VWEU is breed geformuleerd en geeft de Unie - in beginsel - handelingsvermogen en het vermogen om het verschil te maken. Dit is een onderwerp waar de Unie succesvol kan zijn, door een wereldwijd en technologisch ingewikkeld probleem aan

te pakken. Dit is ook essentieel voor de Unie zelf, in een tijdvak waar de steun afbrokkelt voor een EU die meer is dan een gemeenschappelijke markt. De perceptie dat controle is verloren is waarschijnlijk nog sterker op terreinen waar de Europese Unie de centrale actor is.

Deze specifieke opdracht van de Unie is het onderwerp van deze studie. De studie analyseert de bijdragen van specifieke actoren binnen het Europese rechtsbestel. Dit zijn de rechterlijke macht, de EU wetgever, de onafhankelijke toezichthouders, de samenwerkingsmechanismen van deze toezichthouders en, tot slot, de Unie als zodanig in de internationale arena. De legitimiteit en de effectiviteit van de Unie en van het handelen van de verschillende actoren zijn de invalshoeken voor de analyse.

*Algemene conclusies*

De analyse laat zien dat een succesvol gebruik van de bevoegdheden van de Unie op basis van artikel 16 VWEU mogelijk is, in overeenstemming met vereisten van legitimiteit en de effectiviteit. De analyse laat ook zien dat een ambitieuze aanpak nodig is, gelet op de grote uitdagingen van de informatiemaatschappij.

Het succes van de Unie in de uitvoering van haar opdracht is essentieel voor personen wier grondrechten op het spel staan. Het is ook essentieel voor onze democratische rechtsstaten. Daar komt bij dat als de Unie haar ambities kan waarmaken en een effectieve bijdrage kan leveren aan de bescherming van privacy en gegevensbescherming op internet, dit resultaat legitimiteit geeft aan het mandaat van de Unie en - in een wijder perspectief - het vertrouwen in de Unie, dat thans onder druk staat, kan vergroten. Indirect kan dit ook bijdragen aan het vertrouwen in nationale overheden.

Deze studie is optimistisch. De Unie heeft een geschikt mandaat op dit terrein, met - in beginsel - onbeperkte taken voor de rechterlijke macht, de wetgever en de onafhankelijke toezichthouders. Het mandaat maakt ook een succesvolle samenwerking van de toezichthouders mogelijk en stelt de Unie in staat om internationaal effectief te opereren.

Dit optimisme is tevens gebaseerd op de sterke positie van Europa in het internationale domein, gebaseerd op wat wel het Brussels effect wordt genoemd. [1] Het recht kan het verschil maken in de informatiemaatschappij op voorwaarde dat de beschikbare instrumenten op een intelligente manier worden gebruikt.

Het succes van de Unie in de uitvoering van het mandaat voortvloeiend uit artikel 16 VWEU hangt af van de wijze waarop de Unie vereisten van legitimiteit en effectiviteit weet te verzoenen. Een succesvolle uitvoering van het mandaat laat zien dat de Unie in staat is bescherming te bieden op het wereldwijde internet. Kortom, dit is een terrein waar niet alleen het recht, maar ook de Europese Unie het verschil kan maken.

Deze studie stelt dat artikel 16 VWEU erbij gebaat is de begrippen privacy en gegevensbescherming toe te passen met inachtneming van de gewijzigde omstandigheden op

[1] The Brussels Effect, Anu Bradford, 2012, Northwestern University Law Review Vol. 107, No. 1

internet. Ook de verhouding met andere grondrechten, zoals de vrijheid is veranderd door het internet.

In een internet omgeving heeft het niet langer zin privacy en gegevensbescherming als twee te onderscheiden grondrechten te beschouwen. Immers, iedere verwerking van persoonsgegevens kan potentieel de privacy van de burger aan te tasten, in het bijzonder als gevolg van big data. Kortom, deze twee rechten, die in het EU Grondrechtenhandvest worden onderscheiden, maken deel uit van één systeem. Bovendien is op internet gegevensbescherming geen recht die verwerking onmogelijk maakt - het is geen verbodsrecht - maar wel een recht van iedere burger dat zijn of haar gegevens eerlijk worden verwerkt.

Op internet botsen privacy en gegevensbescherming steeds vaker met informatiegrondrechten, dit terwijl de bescherming van eerstgenoemde rechten steeds moeilijker wordt.

Het EU Hof van Justitie houdt in zijn rechtspraak rekening met de noodzaak compensatie te bieden voor het - gepercipieerde - verlies van controle op persoonsgegevens. Het doet dit op basis van de huidige EU wetgeving en in het bijzonder Richtlijn 95/46. De EU wetgever zal spoedig een nieuw wettelijk kader voor gegevensbescherming aannemen, dat wezenlijke vernieuwingen met zich meebrengt en de bescherming naar een hoger plan moet tillen. De EU verdragen erkennen de wezenlijke rol van de toezichthouders die een hoge mate van onafhankelijkheid genieten, zoals ook het Hof heeft bevestigd. De toezichthouders en hun samenwerkingsstructuren spelen een belangrijke rol in de ontwikkeling van de Europese gegevensbescherming. Die rol wordt verder versterkt door het nieuwe wettelijk kader. Tot slot, de Unie speelt een actieve rol in de internationale arena, ook via de bijdragen van de verschillende actoren.

*Specifieke bevindingen, gerelateerd aan de verschillende actoren en rollen*

Artikel 16 VWEU verschaft de Unie een stevig mandaat en verzekert dat privacy en gegevensbescherming per definitie binnen de reikwijdte van het EU recht vallen. De hoge ambities van de Unie zouden compensatie moeten bieden voor het verlies van controle op internet. Echter, de Unie is niet de enige waakhond op internet. Ook de lidstaten moeten een rol spelen. Het Europees stelsel van executief federalisme[2] mag echter niet het beschermingsniveau aantasten.

Een goede uitvoering van het EU mandaat draagt bij aan de sociale legitimatie van de Unie en kan ook een element zijn dat vormt geeft aan het Europees burgerschap. De EU rol moet ook legitiem zijn ten opzichte van de lidstaten. Een effectieve uitvoering geeft de Unie wat output-legitimiteit wordt genoemd. De Unie moet niet alleen de beginselen van privacy formuleren, maar ook zorgdragen voor een effectieve praktijk. Dit vergt een doelmatige instrumentkeuze, die niet alleen de rollen van de verschillende publieke actoren versterkt,

[2] Ontleend aan Koen Lenaerts en Piet van Nuffel, European Union Law, Third edition, Sweet & Maxwell 2010.

maar ook private partijen betrekt bij de uitvoering, waarbij de eindregie overigens wel bij de overheid moet blijven.

Deze studie bevat en aantal suggesties om de verschillende publieke en private te betrekken in het managen van gegevensbescherming. De studie stelt voor om op basis van deze suggesties een strategie te ontwikkelen, waarin ook de verantwoordelijkheden van de verschillende partijen nadrukkelijk worden onderscheiden.

In de laatste jaren heeft het **Hof van Justitie** een belangrijke voortrekkersrol gespeeld, rekening houdend met de impact van de informatiesamenleving. Duidelijke voorbeelden zijn twee arresten uit 2014, *Google Spain* over de verwijdering van zoekgegevens, en *Digital Rights Ireland*, waarbij de richtlijn over het bewaren van communicatiegegevens werd vernietigd. Ook het recente *Schrems* arrest draagt aan dit beeld bij.

Tegen deze achtergrond stelt de studie een eenvoudige taxonomie van grondrechten voor, die het mogelijk maakt een differentiatie te maken in beschermingsniveau, gebaseerd op het belang van een bepaald grondrecht voor de democratische rechtsstaat. Deze taxonomie ziet er als volgt uit:

a. Absolute grondrechten waar geen beperking op mogelijk is. Dit zijn de rechten in titel I Handvest, waardigheid.

b. Rechten met een grote impact op de menselijke waardigheid en de democratie, maar zonder absoluut karakter (zoals privacy en gegevensbescherming).

c. Sociale, culturele en economische rechten. Verdere categorieen zijn de beginselen uit het Handvest (genoemd in artikel 51(2) en 52 (5), de fundamentele vrijheden uit de EU Verdragen en verdere algemene belangen.

De studie onderscheidt vijf oplossingsrichtingen voor de **EU wetgever** om controle te herwinnen. Ten eerste, de bestaande wettelijke instrumenten kunnen worden uitgelegd op een wijze die rekening houdt met de gewijzigde omstandigheden. Ten tweede, de wettelijke arrangementen worden aangepast aan de nieuwe omstandigheden. Ten derde, de gewijzigde verhouding tussen de publieke en de private sector wordt geadresseerd, door de private sector sterker te betrekken bij de implementatie, overigens zonder afbreuk aan de eindregie van de overheid. Ten vierde, de EU en de lidstaten worden gestimuleerd om hun interventies te focussen op wezenlijke elementen van bescherming, om pragmatische redenen en om redenen van internationale rechtsmacht. Ten vijfde, de wetgever stelt de belangrijkste beginselen van gegevensbescherming ter discussie, teneinde de beginselen aan te passen aan de praktijk, maar zonder de behoefte aan bescherming op te geven. Deze vijfde oplossingsrichting is voor de lange termijn, ook al omdat wezenlijke beginselen op verdragsniveau vastliggen.

De bijdrage van de wetgever is essentieel, om controle te herwinnen. Een verordening is het juiste instrument, ook voor de publieke sector. Gegevensbescherming als een recht op eerlijke verwerking vereist dat de wetgever uitvoering geeft aan de belangrijkste beginselen van

bescherming, die in het Handvest zijn opgenomen. De nieuwe verordening past de wettelijke arrangementen aan de nieuwe omstandigheden aan. De verordening laat één ding nadrukkelijk na: de aanpassing van de beginselen.

Deze studie stelt voor dat de EU wetgever een strategie ontwikkelt, gebaseerd op de vijf genoemde oplossingsrichtingen en gericht op de consequentie van internet. Op lange termijn moet zo'n strategie kunnen leiden tot een heroverweging van inhoudelijke beginselen van privacy en gegevensbescherming.

Een essentieel deel van het toezicht is opgedragen aan expert-organen ("expert bodies"), in het bijzonder de onafhankelijke toezichthouders die vooral bekend staan onder het Engelstalige acronym **"DPAs"**. De DPAs zijn onafhankelijke publieke organen – vooral van de lidstaten – met een reeks aan rollen: ombudsman, auditeur, consultant, opleider, beleidsadviseur, onderhandelaar en handhaver. Het mandaat van de DPAs is dus ruim.

De inbedding van de rol van de DPAs in het primaire Europees recht geeft deze organen een constitutionele status in het Europees recht. De studie kwalificeert deze organen als een nieuwe overheidsmacht, gebaseerd op een theorie van Vibert.[3] DPAs ontlenen hun bevoegdheid niet aan de andere overheidsmachten, als agenten ten opzichte van een principaal. In tegendeel, de DPAs zijn zelfs bevoegd toezicht te houden op de andere overheidsmachten, de traditionele trias politica. Deze nieuwe overheidsmacht kan instrumenteel zijn voor het herstellen van vertrouwen, gesteld dat de DPAs opereren in volledige onafhankelijkheid, maar ook binnen een stelsel van checks en balances. DPAs moeten handelen binnen de grenzen van hun bevoegdheid, in overeenstemming met eisen van onafhankelijkheid, effectiviteit en verantwoordelijkheid. Dergelijke eisen gelden ook voor agentschappen, waarvan de DPAs overigens wel moeten worden onderscheiden.

Deze studie stelt voor een model te ontwikkelen voor goed bestuur door de DPAs en geeft de uitgangspunten voor het model, geïnspireerd op de zogenoemde LITER beginselen voor agentschappen, zoals beschreven door Ottow.[4]

De studie presenteert ook drie modellen voor de **samenwerking van DPAs**, te weten: horizontale samenwerking, een gestructureerd netwerk en samenwerking in een Europese DPA. Deze drie modellen vormen een gelaagde structuur voor onafhankelijk, effectief en verantwoordelijk toezicht.

Thans is het toezicht op de naleving van de regels voor gegevensbescherming niet gecentraliseerd op Europees niveau. Hoewel overwegingen van effectiviteit zouden pleiten voor een uniforme en geharmoniseerde aanpak van het toezicht, stelt deze studie geen centralisatie voor, althans niet voor de komende jaren. Geen enkele instelling of adviseur pleitte overigens voor centralisatie tijdens de onderhandelingen over de Verordening gegevensbescherming.

[3] F. Vibert, The Rise of the Unelected, Democracy and the New Separation of Powers, Cambridge University Press 2007.
[4] A. Ottow, Market & Competition Authorities, Good Agency Principles, Oxford 2015, mainly Chapter 3.

De studie pleit wel voor een betere organisatie van het toezicht op privacy en gegevensbescherming in de EU, via de gelaagde structuur. Deze gelaagde structuur heeft niet tot doel delen van het toezicht te centraliseren, maar wel om te verzekeren dat waar het Europees niveau is betrokken, behoorlijke procedures gelden.

**De EU als een actor in de internationale arena** moet verantwoordelijkheid nemen voor globalisering, gebaseerd op de claim dat EU waarden een normatieve waarde hebben en universeel toepasbaar zijn. De EU heeft een wereldwijd gezag dankzij de wettelijke standaarden die deze waarden vertegenwoordigen.

Teneinde effectief bescherming te kunnen bieden op het internet, heeft deze studie de voorkeur voor een unilaterale strategie, met als doel het exporteren van de Europese waarden in het internationale domein. De EU kan daarbij gebruik maken van de faciliteiten die de Raad van Europa biedt, zoals de mogelijkheid dat niet-Europese landen toetreden tot Conventie 108 van de Raad. Als onderdeel van deze unilaterale strategie zouden wel op praktisch niveau bruggen worden geconstrueerd met derde landen die vergelijkbare opvattingen hebben over privacy, zoals de Verenigde Staten.

Daarenboven zou een bilaterale strategie moeten worden geëxploreerd, die is gericht op wederzijdse erkenning, standaardisatie of samenwerking in de handhaving. Deze strategie kan gebaseerd op gemeenschappelijke opvattingen, maar moet ook verschillen accepteren. De OESO zou hierbij een rol kunnen spelen.

Op lange termijn zou een VN-Verdrag de beste bescherming kunnen bieden (de multilaterale benadering). De EU zou initiatieven moeten nemen om het aannemen van zo'n verdrag te bevorderen, met de ambitie om wereldwijd een minimum niveau van gegevensbescherming overeen te komen.

*Tot slot*

Voor de korte termijn vormt de Algemene Verordening Gegevensbescherming een wezenlijke stap voorwaarts, met relevantie voor alle actoren op basis van artikel 16 VWEU.

De verordening lost echter niet alle zwaktes in het systeem op. Het bevalt te bezien of voor de langere termijn de verordening volstaat. Onderwerpen die in elke geval verdere actie vragen voor de langere termijn zijn:

a. De aanpassing van de inhoudelijke beginselen van gegevensbescherming.

b. De fine tuning van de rol van de lidstaten op basis van artikel 16 VWEU.

c. De centralisatie van het toezicht op wereldwijd opererende internet bedrijven.

Deze onderwerpen lenen zich voor academisch onderzoek in de komende jaren.