Can Chinese legislation on informational privacy benefit from European experience?

Zhang, K.

Nederlandse Samenvatting

Samenvatting van: Kan Chinese wetgeving betreffende informationele privacy profiteren van de Europese ervaring?

Dit proefschrift gaat over regelgeving ten aanzien van de bescherming van persoonsgegevens in China. Het primaire doel van mijn onderzoek was om te onderzoeken of het is aan te raden dat China de Europese wetgeving inzake de gegevensbescherming overneemt en implementeert. Ik heb dit onderzoek gedaan vanuit verschillende perspectieven.

In hoofdstuk 2 heb ik, gebruikmakend van relevante documentatie en interviewresultaten, de Europeesrechtelijke materiële persoonsgegevensbeschermingswetgeving vergeleken met het Chinese systeem van kredietregistratie, en heb, vanuit een positivistisch perspectief, van beide het beschermingsniveau beoordeeld. Daarbij heb ik meetinstrumenten gehanteerd die ik heb afgeleid uit de OESO-richtlijnen (versie 2013). De focus lag op de verschillen tussen de twee betreffende rechtsgebieden (en niet op de overeenkomsten). Deze verschillen zijn typerend. Over het algemeen blijkt uit de vergelijking dat de Europese wetgeving betreffende de persoonsgegevensbescherming de beginselen van de informationele privacy zoals ingebed in OESO 2013 veel vollediger dekt dan de Chinese wetten (voor zover die er überhaupt zijn). Er bestaat, aldus beschouwd, een grote kans dat de databank van het Chinese *Credit Reporting Center* (CRC), ware deze operationeel in Europa, illegaal zou worden

bevonden. Ik vestig er de aandacht op dat het CRC met zijn activiteiten drie soorten privacywaarborgen schendt, die alle drie wel zijn opgenomen in de Europese wetgeving. De eerste soort schending betreft de rechten van de betrokkene. Twee elementen uit OESO 2013 zijn vastgelegd in beide rechtsregelingen. Maar daarentegen is het recht om bezwaar te maken, dat kan worden beschouwd als een species van het recht om iets aan te vechten - typerend voor de Europese wetgeving inzake gegevensbescherming - niet opgenomen in de Chinese regelingen. De tweede soort schending betreft de verplichtingen van de voor de verwerking verantwoordelijken. Zo erkent de EU-Richtlijn wel alle OESO-beginselen inzake de verplichtingen van de voor de verwerking verantwoordelijken, terwijl de Chinese Credit Reporting regelgeving de beginselen van gelimiteerd verzamelen, van gelimiteerd gebruik, het transparantiebeginsel en het aansprakelijkheidsbeginsel missen. Dit zijn echt ernstige omissies. De derde soort schending betreft procedurele aspecten. Implementatiebeginselen zijn grotendeels erkend door de Europese gegevensbeschermingswetgeving, met uitzondering van de nationale strategie, die alleen was opgenomen in de OESO-richtlijnen 2013. China echter mist het grootste deel van de procedurele kernaspecten. Er zijn maar drie beginselen te vinden in het Chinese systeem, te weten: "redelijke middelen voor het individu om hun rechten uit te oefenen, adequate sancties en aanvullende maatregelen". Nogmaals, in het licht van OESO 2013 loopt Chinees positief recht inzake gegevensbescherming voor de krediet registratie serieus achter bij Richtlijn 95/46/EG. Daarom kan het gebruik van de Chinese CRC-database vanuit het Chinese rechtssysteem heel goed worden beschouwd als legaal. Vanuit het Europese recht zou datzelfde gebruik echter duidelijk illegaal zijn. Op basis van de bovenstaande vergelijking, concludeer ik dat als de Chinese beleidsmakers Europese gegevensbeschermingswetgeving invoeren, dit vanuit een positivistisch perspectief een verbetering is van de juridische regelingen daarvan in China. Daarom, en uitgaande van de *ceteris paribus* aanname, kan Europese gegevensbeschermingswetgeving dienen als uitgangspunt voor het verbeteren van juridische regelingen in China. Maar aangezien we weten dat *ceteris* niet *paribus* zijn

in Europa en China, merk ik op dat verder onderzoek nodig is waar het gaat om de onderbouwing van de gedachte dat de wetgeving vanuit Europa in China direct kan worden overgenomen en geïmplementeerd.

In hoofdstuk 3 heb ik onderzoek gedaan naar de evolutie van de persoonlijke levenssfeer en de informationele privacy in Europa en in China, aangezien deze verschillende paden hebben gevolgd onder uiteenlopende omstandigheden. Ik begon dit hoofdstuk met een aantal overwegingen over analogieën tussen talen, culturen en rechtssystemen: evenals talen, evolueren juridische systemen ook onder druk van de culturen die ze dienen en waarvan ze deel uitmaken. Door te kijken naar de ontwikkelingen in hun culturele omgeving, kunnen de verschillen tussen de rechtsstelsels beter worden begrepen - zowel het recht in de boeken (*law in the books*, het positivistische perspectief) als het recht in actie (*law in action*, het realistische perspectief). Op basis van mijn analyse concludeer ik dat cultuurverschillen van invloed zijn geweest op de verschillen in gegevensbeschermingswetgeving. Zoals de discussie over Europese wetgeving inzake gegevensbescherming in dit hoofdstuk laat zien, is deze opgekomen vanuit de (functionele) wortels van het Europese privacy-idee dat tot bloei kwam onder de druk van gebeurtenissen in de omgeving. Deze functionele wortels zijn er het eerst, en worden al snel gevolgd door de opkomst van de eerste juridische vormen van wettelijke privacybescherming. Privacyfuncties en -wetten bleven in Europa co-evolueren en culmineerden na de Tweede Wereldoorlog niet alleen in gedetailleerde functionele (en dus instrumentele) wetgeving, maar ook in het tamelijk Kantiaanse idee van privacy als een intrinsiek individualistische menselijke waarde (zoals uitgedrukt in art. 12 UVRM). In China, komt de huidige wettelijke regeling op het gebied van gegevensbeschermingsaangelegenheden rechtstreeks voort uit de Chinese collectivistische cultuur, die alleen het instrumentele aspect van privacy (h)erkent. De bevindingen in dit hoofdstuk ondersteunen de stelling dat de Chinese beleidsmakers zich moeten realiseren dat de Europese gegevensbeschermingswetgeving geenszins wordt overgezet vanuit, noch naar cultureel blanco of neutrale jurisdicties. Zowel Europa als China hebben reeds be-

staande wetgeving inzake gegevensbescherming en hebben reeds gevormde privacy-gerelateerde culturele normen. De culturen waarin de praktijk van de privacy is ingekaderd zijn ingewikkeld en hebben verstrekkende gevolgen voor de manier waarop de wetgeving inzake gegevensbescherming wordt en zal worden begrepen, en voor hoe deze zal worden ontvangen, nageleefd en gehandhaafd. Daarom stel ik voor dat China een voorzichtige benadering volgt waar het gaat om de realisatie van het plan om wetgeving over te nemen.

Aan het einde van hoofdstuk 3 heb ik de verschillen vastgesteld tussen de twee positiefrechtelijke regelingen en de twee betrokken culturen. Er is veel dat op het eerste gezicht een geldige kandidaat lijkt om te worden ingevoerd uit de EU naar China. Maar er zijn ook andere dan culturele risico's. Bijvoorbeeld, zowel technische innovatie als de toepassing van sociale media-diensten zijn zeer dynamisch en hebben de neiging om adequaat wetgeven te bemoeilijken. Om een weloverwogen keuze te maken aangaande wat over te nemen en wat niet, is het nuttig om te analyseren hoe in de betreffende jurisdicties de veerkracht van het ontvangende rechtssysteem wordt ondersteund (of ondermijnd) in een veranderende omgeving. Het is dit punt in het bijzonder dat voor mij de motivatie vormt voor de aandacht die ik in hoofdstuk 4 geef aan de Incomplete Law Theorie.

Teneinde een interpretatie vast te stellen van het fenomeen in kwestie, heb ik voor de analyse de Incomplete Law Theorie van Xu en Pistor benut. Daaruit kwam naar voren dat Europese gegevensbeschermingsregelgeving, zoals Richtlijn 95/46/EG, onvolledig (incomplete) is. De redenen daarvoor vallen in drie categorieën uiteen: ten eerste: de algemeenheid van de richtlijn bemoeilijkt het geven van regels die specifiek genoeg zijn; ten tweede: de technologie, die sterk van invloed is op het onderwerp van de gegevensbeschermingswetten, verandert pijlsnel en maakt daardoor de richtlijn incompleter omdat deze hier ver bij achterblijft; en tenslotte: wetgevers zijn niet in staat om alle mogelijke toekomstige ontwikkelingen te voorzien, ook niet die onvoorziene ontwikkelingen die ontstaan door de massale acceptatie en het gebruik van innovatieve diensten. De technologische veranderingen zijn met name een groot probleem voor de toepasselijkheid op de korte termijn van de richtlijn. Richtlijn 95/46/EG is enige decennia terug ontworpen om gegevensverwerkingstechnologieën te reguleren en is dus gericht op de "oude" problemen, terwijl zich op het vlak van de digitale technologieën radicale omwentelingen hebben voorgedaan. Nieuwe geavanceerde digitale technologieën hebben hun intrede gedaan in publieke communicatienetwerken en in de samenleving. Toegang tot digitale mobiele netwerken is beschikbaar en betaalbaar geworden voor het grote publiek. De digitale netwerken bieden enorme mogelijkheden voor de verwerking van persoonsgegevens. Al deze veranderingen vereisen daarom frequente aanpassingen van de wet wil deze effectief blijven. Dit heeft geleid tot problemen met het aan blijven passen van de focus en werkbaarheid van de wet aan de realiteit.

Wat deed Europa aan de hieruit voortkomende onvolledigheid? Europese beleidsmakers creëerden een nieuwe functie, die van een "autoriteit voor gegevensbescherming" die aanvullende regelgevende- en rechtshandhavingsbevoegdheden (LMLEP, law making and law enforcing powers) kreeg toebedeeld, om te kunnen ingrijpen bij het terugdringen van problemen die worden veroorzaakt door de onvolledigheid. In hoofdstuk 4 ga ik nader in op de Artikel 29 Werkgroep en de nationale autoriteiten voor gegevensbescherming die zo een belangrijke rol spelen bij de regulering en rechtshandhaving met het oog het verminderen van de onvolledigheid. Het onderzoek bevestigde dat de komst van deze autoriteiten een reactie vormde op het handhavingsprobleem dat werd veroorzaakt door het zeer onvolledige recht. De gegevensbeschermingsautoriteiten zijn flexibeler dan de wetgevers bij het kunnen aanpassen van de wet aan een veranderde technische omgeving (alhoewel de omvang van hun wetgevingsbevoegdheid beperkt is), omdat de korte tijd die zij nodig hebben om te reageren hen beter in staat stelt om het snelle tempo van de technologie bij te houden. En gegevensbeschermingsautoriteiten zijn meer pro-actief dan rechters, omdat ze acties kunnen initiëren om de gegevensbescherming te handhaven in situaties waarin rechters nu eenmaal moeten wachten tot er een geding wordt aangespannen. Op basis van de bevin-

dingen van hoofdstuk 4 wordt dan ook de veronderstelling (die Chinese beleidsmakers koesteren) verworpen dat de Europese wetgeving inzake gegevensbescherming volledig zou zijn en dat het ontwerp beperkt kan blijven tot de overname van de positieve materiële rechtsregels inzake gegevensbescherming. Ik toon aan, anders dan de verwachtingen daaromtrent, dat de problemen van de technologische dynamiek en het massale gebruik van sociale media niet triviaal zijn en dat deze om maatregelen vragen die garanderen dat er een uitstekend geïnformeerde en zeer toegankelijke "autoriteit" beschikbaar is met toereikende LMLEP om in de gaten te houden dat de onvolledigheid van de wet niet onhoudbaar wordt. Ik concludeer dat de juridische overname, zoals wordt beoogd, geen effectieve gevolgen zal hebben, tenzij er ook ruimte wordt gecreëerd voor een competente regelgevende autoriteit.

Als follow-up van deze conclusie heb ik in hoofdstuk 5 geanalyseerd met welke verschillen tussen law in the books en law in action de gegevensbeschermingsauthoriteiten van de EU worden geconfronteerd wanneer ze te maken krijgen met het Amerikaanse Facebook en met RenRen, het Chinese broertje daarvan. Het blijkt overduidelijk dat de huidige praktijken van RenRen niet in overeenstemming zijn de beginselen van de Europese gegevensbescherming, en ook niet met de EU gegevensbeschermingswetgeving. Dit betekent dat als RenRen zijn EU-hoofdkwartier in enige lidstaat in Europa zou openen, de onderneming meervoudige klachten over de gegevensbescherming kan verwachten. Wat Facebook betreft concludeer ik dat - ook al lijken de huidige praktijken de EU-wetgeving inzake gegevensbescherming na te leven – dit niet helemaal opgaat wat betreft de beginselen van de Europese gegevensbescherming. Dit leidt tot het inzicht dat wat aanvaardbaar is gezien de EU-privacywet niet aanvaardbaar behoeft te zijn vanuit de visie van de beginselen van de Artikel 29 Werkgroep. Aan de ene kant betekent dit dat het niveau van de bescherming van betrokkenen kan stijgen naar een aanzienlijk hoger niveau, afhankelijk van de uitvoering door betreffende autoriteiten (als die autoriteiten zitting hebben in de Werkgroep). Aan de andere kant toont dezelfde bevinding aan dat het moeilijk is strikte naleving van de wet af te dwingen

met het doel om het gedrag inzake de gegevensbescherming van een wereldwijd toonaangevend Social Network Service speler als Facebook te beïnvloeden. Met andere woorden, de effectiviteit van de law in action is complex en moeilijk te voorspellen door de wet en degenen die de wet handhaven geïsoleerd te bekijken. In China, wordt de spanning tussen de effectiviteit van de law in action en de optimale kwaliteit van juridische constructies groter, althans bij de aanvang van het plan tot overname van de gegevensbeschermingsregels. De onvolledigheid van de wetgeving inzake gegevensbescherming is in China erger dan in Europa, omdat veel van dergelijke wetten er eenvoudigweg helemaal niet zijn en de meeste van dergelijke wetten die wel bestaan onlangs pas zijn ingevoerd. De onvolledigheid is ook ernstiger in China dan in Europa, omdat wetshandhavingsinstanties eenvoudigweg de ervaring missen van het rechtspreken met aanzienlijke aantallen en verscheidenheid van de gevallen. Dit is met name relevant voor de uitvoering onder de auspiciën van het *Ministry of Industry and Information Technology*, het MIIT. Om verschillende redenen kan van het MIIT qua rechtshandhaving geen effectiviteit worden verwacht, althans niet in de beginfase van de ontwikkeling van de gegevensbeschermingsinstituties. Zo worden de Chinese wetgevers geconfronteerd met een uiterst lastige situatie: ze moeten echt nodig een Europese soort van gegevensbescherming ontwikkelen, en toch missen ze het instrumentarium om dat te doen. Erger nog, een pasklaar recept voor rechtshandhaving zoals dat in het verleden elders heeft gewerkt, kan China op de korte en middellange termijn niet helpen.

Ik ben op een punt aangekomen dat ik in staat ben om mijn onderzoeksvraag: "Is China's overnameplan aan te raden?" kan beantwoorden. Met mijn benadering kom ik tot de conclusie dat het niet haalbaar is om uitsluitend de EU-wetgeving inzake gegevensbescherming over te nemen (zoals voorgesteld in het overnameplan van China), tenzij een equivalent van de EU-gegevensbeschermingsautoriteiten in dat plan wordt meegenomen. Chinees gegevensbeschermingsrecht is minder krachtig dan het EU-privacyrecht (hoofdstuk 2). Echter, culturele verschillen (hoofdstuk 3) en inherente onvolledigheid van het

EU-recht (hoofdstuk 4), in combinatie met het feit dat institutionele EU-regelingen die de onvolledigheid verminderen niet zullen werken in China (hoofdstuk 5) doen me besluiten dat de effectiviteit van een geïmporteerde Europese gegevensbeschermingswetgeving niet te veel kan worden verwacht.

In het tweede deel van mijn onderzoek verken ik welke extra mogelijkheden kunnen worden gevonden vanuit het perspectief dat wordt geboden door de complexiteitstheorie, als het onderwerp van de gegevensbeschermingsregelgeving wordt beschouwd als een complex adaptief systeem (hierna: CAS). Voor deze verandering van perspectief is gekozen omdat de fenomenen waarmee ik geconfronteerd werd in de hoofdstukken 3-5 die kenmerkend zijn voor de rechtsbescherming van persoonsgegevens kunnen worden samengevat met behulp van zes karakteristieken. Wie persoonsgegevens gebruiken (produceren en benutten) vormen een netwerk, worden onderling afhankelijk, en vertonen zo nu en dan pad-afhankelijk, dynamisch, complex en adaptief gedrag. In dit tweede deel, identificeer ik eerst het onderwerp van de wetgeving inzake persoonsgegevensbescherming als een PDC (Personal Data Community). Daarna onderzoek ik via het combineren van de PDC met de kennis en ervaringen uit verschillende klassen van CAS, of het onderwerp van de wetgeving inzake gegevensbescherming als een netwerk van gebruikers van de gegevens de kenmerken vertoont van een CAS en wat dit betekent voor de toekomst van de wetgeving inzake gegevensbescherming. Met behulp van enkele belangrijke CAS-eigenschappen en door deze te relateren aan onze PDC en de daarbij bijbehorende ecologie, stel ik vast dat deze eigenschappen gelden voor de PDC en dat dus de PDC kan worden opgevat als een CAS. Vanuit het CAS-perspectief is de door de mens geschapen PDC een groot en dynamisch systeem van interactieve gegevensgebruikers in een netwerk met een bepaald organisatiepatroon van waaruit het vermogen ontstaat tot aanpassing aan interne en externe veranderingen door zelf-organisatie, emergentie en co-evolutie/leren. Mijn bevindingen daagden mij uit tot het maken van juridische constructies op het gebied van gegevensbescherming, en zo te proberen een CAS te "temmen". Bewijs ontleend uit case studies weergegeven in dit boek, even-

als in andere bronnen veronderstellen dat de materie van de wetgeving inzake gegevensbescherming (mogelijk) erg verschilt van dat van andere rechtsgebieden. Het kijkt namelijk op voortdurende kritische overgangssituaties in de praktijk. Zodoende – nu we voortdurend situaties moeten reguleren, die de wetgever zich niet kon voorstellen en zich ook niet heeft voorgesteld toen hij de wet ontwierp – vereisen de doelstellingen van de wetgeving inzake gegevensbescherming, de redenen van haar bestaan en de modaliteiten van deze regelgeving methoden die nogal verschillen van die met een focus op de interpretatie van het materiële recht zoals bij de andere rechtsgebieden. Ik stel voor dat de toekomstige wetgeving inzake gegevensbescherming met vrucht kan worden geconstrueerd op de aanbevelingen van de CAS-theorie: zoals Ruhl (1997) ons leert, kunnen de problemen die zich in een CAS voordoen alleen worden aangepakt, tenzij je denkt als een complex adaptief systeem. Dus het probleem dat aandacht vereist is om ervoor te zorgen dat de wetgeving inzake gegevensbescherming is afgestemd op wat het is.

Maar hoe?

De multidisciplinaire CAS-theorie kan de rechtswetenschap helpen om de wetgever beter te informeren over te verwachten risico's en resultaten van wetgevende activiteiten die naar CAS-elementen verwijzen. In het tweede deel stel ik een aantal strategieën voor die kunnen worden ingezet om juridische onderzoekers te helpen om regulerende kaders te vinden voor complexe adaptieve fenomenen in de PDC. Deze strategieën omvatten onder meer: (i) de voortdurende en herhaalde evaluatie van feitelijke en verwachte effecten van wetswijzingingen; (ii) aandacht voor de culturele en economische omgeving; (iii) begrip voor de functionele betekenissen van "hubs," (iv) kennis van en aandacht voor al dan niet bewuste menselijke drijfveren en (v) aandacht voor de wijzen waarop drijfveren en aangeleerde normen op elkaar reageren.

Ik denk dat de rechtswetenschap de eigen identiteit en de begrenzingen ervan in multidisciplinaire verbanden expliciet moet maken en verdedigen door erop te hameren dat voor de rechtswetenschap het autonome keuzegedrag van verantwoordelijke individuen centraal staat – gedrag waarbij rekening kan

worden gehouden met juridische en culturele normen, kortom gedrag dat bewust is en moet zijn aangeleerd. Dit is bijvoorbeeld anders voor de sociale wetenschappen waarin veelal gezocht wordt naar kennis over mechanismen die het menselijk keuzegedrag (ook onderbewust) kunnen sturen. Ik meen dat een wetgever vanuit beide wetenschappelijke perspectieven moet worden geïnformeerd, liefst consistent ingekaderd. Ik meen dat complexiteitstheorie zo'n inkadering kan bieden.

Het beeld van het onderwerp van de wetgeving inzake gegevensbescherming als een CAS is een voortdurende in plaats van een voltooide constructie. Ondanks het feit dat onze inzichten in de CAS-theorie zich in een staat van evolutie bevinden, hebben de inspanningen tot nu toe al gediend om het begrip te verdiepen van de vele problemen die de wetgeving inzake gegevensbescherming bemoeilijken. En zij hebben gewerkt als kritische factor op een aantal fouten van de huidige gegevensbeschermingswetten. Het is tegen deze achtergrond dat ik verwacht dat de regulering van gegevensbeschermingsitems kan gaan profiteren van de informatie die kan worden verkregen door te kijken door de bril van de CAS-theorie.