Concept, versie 0.97.

Goede code

De digitale samenleving in balans

Jaap-Henk Hoepman, Theo Hooghiemstra[1]

1. Inleiding

Onze geschiedenis laat een constante strijd tussen de burgers en hun bestuurders zien als het gaat om het beschermen van de grondrechten aan de ene kant, en om het verhogen van de veiligheid en van de efficiëntie en slagkracht van het bestuur aan de andere kant. Dit is in de digitale samenleving niet anders. In het digitale domein woedt echter ook een andere strijd: die tussen de vraag of techniek de wet zou moeten voorschrijven ('code is Law') of de wet de techniek[2] ('law is code'[3]). Het 'code is law' kamp verklaart de normen en waarden zoals die door systeemarchitecturen als 'emergent behaviour'[4] ontstaan superieur. Het 'law is code' kamp vindt daarentegen dat het vanuit het perspectief van de democratische rechtsstaat wenselijk is dat ICT ondergeschikt is aan wet- en regelgeving. Vanuit deze visie is het wenselijk dat de wetgever zich gaat verdiepen in de mogelijkheden die de techniek biedt om rechtsnormen te implementeren in de vorm van 'juridische bescherming by design'.[5]

---

[1] Dr. Jaap-Henk Hoepman is senior onderzoeker bij TNO en Universitair Hoofddocent bij de Radboud Universiteit Nijmegen, Mr. drs. Theo Hooghiemstra is MT-Lid voor Onderwijs, Cultuur, Welzijn en Zorg bij PBLQ.

[2] Bart Jacobs, De computer de wet gesteld, oratie mei 2003.

[3] Lessig, L., Code and Other Laws of Cyberspace, New York 1999 en recenter: L. Lessig, Code version 2.0, New York: Basic Books 2006.

[4] Emergent behaviour is gedrag dat slechts voorspeld kan worden via analyse van een systeem als een geheel.

[5] Zie Hildebrandt, M., Juridische bescherming 'by design'?, Rechtsfilosofie & Rechtstheorie 2010 (39)2, p.101 – 106.

In dit artikel willen we laten zien dat deze twee principes meer met elkaar te maken hebben dan op het eerste gezicht lijkt. Sterker nog, wij pleiten in dit artikel voor *goede code*[6] om de digitale samenleving in balans te brengen: code gebaseerd op het 'code is law' principe, maar als resultaat van een democratisch beslisproces en in wisselwerking met de juridische afbakening ('law is code').

Het artikel bestaat uit vijf delen. Na deze inleiding beschrijven wij het spanningsveld tussen stuwende beginselen (zoals veiligheid en efficiëntieverhoging) en verankerende beginselen (zoals privacy en keuzevrijheid) overeenkomstig het rapport iOverheid van de WRR[7]. Bij de politiek en beleidsmakers lag dit spanningsveld tot voor kort onder de radar. Voor een zorgvuldige keuze tussen stuwende en verankerende beginselen zijn procesbeginselen zoals transparantie, noodzakelijk. Het derde deel gaat over goede code. Wat is noodzakelijk en mogelijk om te komen tot goede code? Welke ontwerpprincipes dienen daarbij te gelden? Het vierde deel beschrijft het proces om tot goede code te komen en ten slotte eindigen we met conclusies.

Wij behandelen bovenstaande vragen aan de hand van het elektronisch patiëntendossier en persoonlijke gezondheidsdossiers als casuïstiek. Dit artikel laat zien dat goede code essentieel is, zowel in technische als juridische zin. Van belang is daarbij dat meer (wetgevings)juristen en technici expertise opdoen over de relatie tussen recht en ICT-architectuur. Hopelijk draagt dit artikel bij aan een dialoog tussen technici en juristen over de wisselwerking tussen techniek en recht, met als doel om gezamenlijk als juristen en technici te komen tot 'goede code'.

2. Het spanningsveld

2.1. Beginselen en grondrechten

In het rapport iOverheid geeft de WRR een analyse van de wijze waarop de overheid zicht de afgelopen decennia van een technologie-gedreven e-overheid heeft ontwikkeld tot een informatiegestuurde overheid. Achter de veelal door veiligheid, effectiviteit en efficiency gedreven digitalisering heeft zich haast sluipenderwijs een verknoping en vernetwerking van informatie voorgedaan, die de relatie tussen burger en overheid wezenlijk verandert. Het WRR-rapport spoort de overheid aan te beseffen een iOverheid te zijn, en tegenover de stuwende beginselen als veiligheid en efficiency, verankerende en procesmatige beginselen te stellen die deze stuwende beginselen als het ware in toom houden.

---

[6] We bedoelen hier met "code" een code in technische zin, zoals softwarecode.

[7] Wetenschappelijke Raad voor het Regeringsbeleid, iOverheid Rapport nr. 86, (WRR, 2011).

De verankerende beginselen staan voor het waarborgen van grondwettelijke vrijheden en zelfbeschikking van het individu. Privacy en keuzevrijheid zijn voorbeelden van verankerende beginselen die de WRR noemt en die we in dit artikel nader uitwerken.

De procesmatige beginselen zijn er op gericht het spanningsveld tussen de stuwende en verankerende beginselen expliciet te maken. Effectiviteit dient zo geregeld te zijn dat geen disproportionele privacy-inbreuken plaatsvinden. Artikel 8 EVRM stelt als voorwaarden voor een gerechtvaardigde privacy inbreuk in het tweede lid: "de inbreuk moet noodzakelijk zijn in een democratische samenleving en proportioneel aan het nagestreefde doel". Gelet hierop is effectiviteit van een maatregel die de privacy schendt zelfs een vereiste: een maatregel die niet effectief is kan nooit noodzakelijk zijn.

Transparantie en accountability zijn volgens de WRR voorbeelden van procesmatige beginselen. Overigens merkt Dommering[8] terecht op dat transparantie al een onderdeel is van het privacyrecht, zie bijvoorbeeld de artikelen 33, 34 en 35 van de Wet bescherming persoonsgegevens (Wbp), terwijl accountability van toepassing is op het hele proces (stuwend, verankerend en procesmatig)

2.2. Onder de radar

Het spanningsveld tussen de stuwende en verankerende beginselen bevond zich bij de op elektronische dienstverlening gerichte 'eOverheid' lange tijd grotendeels onder de politiek-bestuurlijke radar. Politiek en beleid hebben tot op heden weinig oog gehad voor een zich ontwikkelende praktijk waarin samenhangende informatiestromen het karakter van de overheid domineren. De casuïstiek over de 'informatiestromen' waarin burgers verstrikt raken in machts- en welzijnssystemen die door de overheid worden aangestuurd is omvangrijk[9]. De voorstudies van het iOverheid-rapport brengen de bekendste gevallen in beeld: het Schengen Informatiesysteem[10], het EPD[11], het EKD, de Verwijsindex Risicojongeren[12] en

---

[8] Dommering E., Het bestuur als tovenaarsleerling van ICT, Nederlands Juristen Blad, 13-01-2012, afl. 2, p.112.

[9] Dommering E., Het bestuur als tovenaarsleerling van ICT, Nederlands Juristen Blad, 13-01-2012, afl. 2, p.110.

[10] Broeders D , Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa, in: D.Broeders, C.M.K.C.Cuijpers & J.E.J.Prins red.) De staat van informatie, WRR-verkenning nr. 25, 2012, Amsterdam: Amsterdam University Press

[11] Pluut B. Het landelijk EPD als blackbox. Besluitvorming en opinies in kaart. WRR-webpublicatie nr. 45, 2010, www.wrr.nl.

Veiligheidshuizen[13]. Het Rathenau Instituut liet dit in 2010 al zien in het rapport 'Check in/Check out' over de digitale ruimte. Ook het overzicht in figuur 1.1. van het iOverheid-rapport van de instanties waarmee de Belastingdienst gegevens uitwisselt met behulp van het BSN is illustratief.[14] Deze informatiestromen kunnen vergaande gevolgen hebben voor de bescherming van grondrechten, zoals non-discriminatie en privacy. In het navolgende werken we de mogelijke gevolgen voor het grondrecht 'privacy' en het beginsel van keuzevrijheid als voorbeeld uit..

2.3. Privacy: de techniek als veroorzaker en mogelijke oplossing

Met privacy bedoelen we in dit artikel in algemene zin het grondrecht op eerbiediging van de persoonlijke levenssfeer zoals vastgelegd in artikel 10 van onze Grondwet. Dit algemene recht wordt in de Grondwet uitgewerkt in een aantal specifieke bepalingen die de wetgever opdragen om 'ter bescherming van de persoonlijke levenssfeer' bepaalde regels te stellen in verband met het vastleggen van persoonsgegevens. Deze uitwerking is – overeenkomstig Richtlijn 95/46/EG – vertaald in de Wet bescherming persoonsgegevens (Wbp). Privacy in de door ons bedoelde zin wordt beïnvloed door technologische ontwikkelingen. Aan het eind van de 19e eeuw bijvoorbeeld baarde de opkomst van de fotografie en de verspreiding van kranten en (roddel)bladen grote zorgen[15].

Het grondrecht privacy staat onder druk. Bijvoorbeeld doordat persoonsgegevens die voor dienstverlening zijn verzameld vervolgens gebruikt kunnen worden voor controle, opsporing en handhaving. Hildebrandt stelt dat het doelbeperkingsbeginsel haaks lijkt te staan op alles waar de computationele ondergrond van cyberspace voor staat: dataverzameling is interessant omdat het nieuwe kennis oplevert waarvan de toegevoegde waarde pas achteraf kan blijken.[16] Zij laat vervolgens zien dat ook andere beginselen en grondrechten, zoals gelijke

---

[12] Keymolen E.en J.E.J. Prins 'Jeugdzorg via systemen. De Verwijsindex Risicojongeren als spin in een digitaal vangnet' in D. Broeders, C.M.C.K. Cuijpers & J.E.J. Prins (red) De staat van informatie, WRR-Verkenning nr. 25, 2011, Amsterdam. Amsterdam University Press.

[13] Holvast J. en M.J. Bonthuis Blackboxonderzoek Veiligheidshuizen, WRR-webpublicatie nr. 49, www.wrr.nl.

[14] Wetenschappelijke Raad voor het Regeringsbeleid, iOverheid Rapport nr. 86, (WRR, 2011).p. 28.

[15] Warren S. en Brandeis, L. The right to privacy. The implicit made explicit. Harvard Law Review, IV (5), December 15, 1890, 193–220.

[16] M. Hildebrandt, De rechtsstaat in cyberspace, Nijmegen: uitgegeven in eigen beheer 2011, p.21.

behandeling en het recht op tegenspraak op gespannen voet staan met de manier waarop cyberspace zich nu ontwikkelt.

Tot op heden is bij de inrichting van informatiesystemen in de publieke sector vrijwel geen aandacht besteed aan het op voorhand afdwingen van Wbp-normen. Het inzetten van technologie om juist grondrechten te waarborgen heeft nog steeds amper aandacht in het publieke domein. Dit ondanks het feit dat al tijdens de parlementaire behandeling van de Wbp de Tweede Kamer unaniem de motie Nicolaï[17] aannam, op basis waarvan de publieke sector het goede voorbeeld zou geven door stimulering van het gebruik van zogenaamde Privacy Enhancing Technologies (PETs) in de zin van artikel 13 van de Wbp. PETs zijn te definiëren als een samenhangend geheel van ICT maatregelen dat de persoonlijke levenssfeer (conform de EG richtlijn 95/46 en de Wbp) beschermt door het elimineren of verminderen van persoonsgegevens of door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens. Een en ander zonder verlies van de functionaliteit van het informatiesysteem waarbinnen zij worden toegepast.[18] PETs zijn dus een onderdeel van een overkoepelende *privacy by design* methodiek, inclusief *privacy impact asssessments* (PIA's), waarbij privacy requirements al bij het ontwerp van het systeem worden meegenomen. Zij worden niet alleen technisch, maar ook procedureel verankerd.[19] Merk op dat we PETs niet zien als een toevoeging aan een al bestaande applicatie om, achteraf, de privacy impact van de applicatie in te perken. Dat zou namelijk niet werken. In plaats daarvan beschouwen we PETs als de basisbouwblokken die gebruikt worden bij het ontwerpen en bouwen van privacyvriendelijke systemen.

Er is een taakverdeling nodig tussen technische, juridische en organisatorische oplossingen. Technische oplossingen kunnen behulpzaam zijn om juridische en organisatorische oplossingen te vinden, maar zij kunnen niet alle vraagstukken oplossen die voortvloeien uit de afweging tussen stuwende en verankerende beginselen. Wat betreft de juridische oplossingen is overigens interessant dat artikel 23 van de voorgestelde EU-verordening Gegevensbescherming *privacy by design and by default* verplicht stelt[20]. Dat betekent dat standaardinstellingen moeten worden gehanteerd die de betrokkene het meeste bescherming geven van zijn privacy. Een verordening mag niet, zoals de huidige richtlijn, door een lidstaat

---

[17] Tweede Kamerstukken 1999-2000, 25 892, nr. 31.

[18] Zie Hooghiemstra, T.F.M., Privacy bij ICT in de zorg, College bescherming persoonsgegevens, Den Haag, november 2002, p. 46.

[19] Zie voor PETs bij een ziekenhuisinformatiesysteem J.J. Borking, Privacyrecht is code, 2010, p.265-269 en Klaver 2002, p.51 en Koorn, Deventer, 2004

[20] Proposal for a Regulation (EC), General Data Protection Regulation. Brussels 25.1.2012, com(2012) 11 final

naar eigen inzicht worden geïmplementeerd. De lidstaten mogen slechts uitvoeringsmaatregelen treffen, zoals het aanwijzen van toezichthouders en het voorzien in adequate sancties. Als de verordening wordt aangenomen, worden *privacy by design* en *privacy by default* Europees de norm. De lidstaten behouden weliswaar hun 'margin of appreciation', maar die is veel beperkter dan de implementatievrijheid bij de huidige Richtlijn. Wel moet worden opgemerkt dat het hier natuurlijk om een zeer open norm gaat, die nader uitwerking vergt in "best practices" en handreikingen om de voorgestane privacybescherming ook (letterlijk) tot zijn recht te laten komen.

Niettemin kan de voorgestelde verordening een impuls geven aan het Nederlandse beleid op het gebied van inzet van PET's. Tot nu toe kwam dat maar matig uit de verf. Het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties liet na de inwerkingtreding van de Wbp[21] een paar onderzoeken doen[22] en vervolgens een Witboek[23] opstellen, maar in de praktijk is daar tot op heden vrijwel niets mee gedaan. Zo is de inzet van PETs bij het EPD gebleven bij een initiatief bij psychiatrisch ziekenhuis Veldwijk, na een privacy-audit van de toenmalige Registratiekamer. Dat kan beter, ook al moet ervoor gewaakt worden dat PET's af te schilderen als panacee voor alle privacykwalen; het blijft uiteraard een hulpmiddel.[24]

Bovendien hoeft de inrichting van een informatiesysteem niet alleen tot het waarborgen van de verankerende grondrechtelijke beginselen te leiden via het afremmen van de stuwende beginselen, maar kan de inrichting van een informatiesysteem juist bevorderen dat gewenste functionaliteit geleverd wordt. In de volgende paragrafen werken we uit hoe de inrichting van een informatiesysteem kan waarborgen dat de gewenste doelen bereikt worden zonder afbreuk aan privacy-principes.

---

[21] 1 september 2001

[22] Horlings E, M. Botterman, E. Frinking, R. Hamer, A.Lierens, L.Valeri & M. van de Voort, Werkbare vormen van Privacy Enhancing Technologies, Den Haag 2003

[23] Koorn R., H. van Gils, J. ter Hart, P.Overbeek, R. Tellegen en J.J Borking, Privacy Enhancing Technologies, Witboek voor Beslissers, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag 2004.

[24] Zie Hildebrandt, M., Juridische bescherming 'by design'?, Rechtsfilosofie & Rechtstheorie 2010 (39) 2, p.105.

2.4. Keuzevrijheid en informationele zelfbeschikking

Het tweede voorbeeld van een verankerend beginsel dat volgens de WRR tot op heden in de politiek bestuurlijke belangenafweging (te) vaak onder de radar is gebleven is keuzevrijheid. In de wereld van recht en ICT gaat het daarbij tevens om wat het Bundesverfassungsgericht in 1983 in de Census case[25] "informationele zelfbeschikking" noemde. Dat wil zeggen: het recht van ieder individu om – afhankelijk van de context – te besluiten over de ontsluiting en het gebruik van gegevens in relatie tot hemzelf. Het Hof zag dit recht als een basisingrediënt voor een individu om relaties op te bouwen met andere personen en organisaties in een samenleving die in toenemende mate afhankelijk is van moderne ICT. Het betreft overigens een relatief recht. Enerzijds omdat mensen niet altijd juridisch en praktisch zelf mogen bepalen of hun naam gebruikt wordt en anderzijds omdat de bescherming van het grondrecht privacy niet alleen op de schouders van individuele burgers gelegd kan en mag worden.

Op Europees niveau is het recht op informationele zelfbeschikking zeker niet expliciet omarmd. Nergens in het Europees Verdrag, noch in de EU-richtlijn voor gegevensbescherming is er een directe verwijzing naar informationele zelfbeschikking.

Het is verder ook alleen Duitsland dat een grondrecht op 'Algemeine Handlungsfreiheit' kent.[26] Maar zelfs in Duitsland wordt nergens vastgesteld wat die keuzevrijheid in de praktijk precies inhoudt. Mede ten gevolge van de nieuwe media hebben we een overdaad aan keuzes. In hoeverre de burger die keuze- en informatievrijheid kan aanwenden komt aan de orde bij het onderwerp persoonlijk gezondheidsdossier in paragraaf 4.

2.5. Boven de radar: transparantie?

Het is een verdienste van het WRR-rapport dat het laat zien dat in empirische zin een iOverheid is ontstaan zonder dat deze op politiek-bestuurlijk niveau is ontworpen en dat het 'waarschuwingsvlaggen' zet bij informatieverwerkende processen die de aandacht verdienen van een overheid die zorgvuldig met zijn burgers wenst om te gaan. Dat begint ermee dat in het spanningsveld tussen de genoemde beginselen steeds expliciet gemaakt dient te worden wat informatiesystemen in de publieke sector wel of niet moeten kunnen? Dit houdt onder andere in dat bij het opstellen van de ontwerp-eisen rekening gehouden dient te worden met de juridische specificaties, zoals die bijvoorbeeld voortvloeien uit de Wbp. Curvers en Schmidt noemen dit *legal requirements engineering*. [27]

---

[25] BverfG 15 december 1983, NJW 1984, 419

[26] Haratsch, A., Allgemeine Handlungsfreiheit, blz. 558-572 in: S.M. Heselhaus & C.Nowak, Handbuch der Europaischen Grundrechte, Munchen: Beck.

[27] S. Curvers & A. Schmidt, Aanbesteding en innovatie, een inleiding in Legal requirements engineering, Leiden, 2008, p. 129.

Om tot een zorgvuldige en expliciete keuze te komen zijn de eerdergenoemde procesbeginselen van belang. Het transparantiebeginsel is enerzijds noodzakelijk om politieke en beleidsmatige keuzes te kunnen volgen en beïnvloeden. Het rapport iOverheid betoogt dat door ongecontroleerde groei van gegevensuitwisseling burgers en bedrijven geen zicht meer hebben op wat de overheid van ze weet of juist verstrikt kunnen raken in de informatiekluwen.

Anderzijds is transparantie noodzakelijk om individuele (vrijheids)rechten ten volle uit te kunnen oefenen. Het rapport iOverheid laat ook zien dat de publieke sector tot op heden niet goed in staat is de kansen te benutten die een verdergaande digitalisering biedt. Technologie kan bijvoorbeeld in de gezondheidszorg behulpzaam zijn bij het verlenen van digitaal inzagerecht betreffende iemands eigen gegevens of bij het mogelijk maken van patiëntenportalen en persoonlijke gezondheidsdossiers.[28]

Digitaal inzagerecht op grond van artikel 35 Wbp of artikel 7:456 BW via portalen en persoonlijke dossiers zijn mooie stappen op weg naar zelfbeschikking en transparantie voor de patiënt. Dat aan deze geschreven regels echter beperkingen kleven laat Mireille Hildebrandt zien aan de hand van artikel 35 Wbp. In dat licht scoort de pendant van dit artikel in de Duitse Datenschutsgesetz beter.[29] Voor zover geschreven recht echter tekort schiet én niet verder verbeterd kan worden werken we in de volgende paragraaf de vraag uit in hoeverre juridische bescherming als default ingebouwd kan worden in de architectuur in de vorm van “goede code”.

3. Goede code

3.1. Code is law

Zoals we bij de bespreking van het onderwerp PET’s al zagen kan technologie als hulpmiddel worden ingezet om onze privacy te beschermen. Net zo goed als dat er technieken bestaan die de veiligheid van een systeem verhogen (smart cards, het gebruik van access control, encryptie), zo bestaan er technieken die de privacy beschermen, zoals het scheiden van identiteitsdomeinen en de inzet van Trusted Third Parties (TTP’s). Privacybescherming moet dan wel een expliciete keuze zijn, die aan het begin van het ontwerpproces wordt gemaakt en meegenomen in het ontwerp van het systeem.

---

[28] Zie voor een juridisch en empirisch overzicht inzake patiëntenportalen en persoonlijke gezondheidsdossiers, Hooghiemstra, T.F.M. en J. Nouwt, eHealth en Recht. Inleiding op het thema, Computerrecht, aflevering 6, december 2011, p. 288-289.

[29] M. Hildebrandt, De rechtsstaat in cyberspace, Nijmegen: uitgegeven in eigen beheer 2011, p.23

De architectuur van een systeem is daarvoor essentieel. Deze bepaalt namelijk niet alleen hoe een systeem op dit moment functioneert, maar ook hoe het zich in de toekomst kan ontwikkelen. Een architectuur schept mogelijkheden, maar kadert ook in. Het is in zekere zin een abstracte benadering van hoe de wereld (in ieder geval de wereld waar het systeem in opereert) in elkaar zit. Niet alleen in descriptieve zin, maar zeker ook in normatieve zin. Architectuur is in die zin vergelijkbaar met wetgeving. Niet voor niets noemde Lawrence Lessig het boek waarin hij zijn ideeën uitwerkte "*Code, and other laws of cyberspace*"[30]. Code staat hier onder andere voor architectuur en software. Er is echter een cruciaal verschil tussen architectuur aan de ene kant en wetgeving aan de andere kant. Wetgeving is aan verandering onderhevig. Voor architectuur geldt dit niet. Die is min of meer onveranderbaar. Weliswaar zal een architectuur een zekere flexibiliteit in de realisatie en ontwikkeling van het systeem mogelijk maken, maar de essentie van de architectuur, het raamwerk, blijft onveranderd. Plat gezegd: een bungalow wordt nooit een wolkenkrabber, maar je kunt er altijd wel een serre aanbouwen. De architectuur is de kern van het hele systeem en kan dus alleen veranderd worden door het systeem volledig te vervangen door een nieuw systeem. Bij substantiële verandering van de wet kan dat betekenen dat het hele systeem vervangen moet worden.

3.2. Voorbeelden

Een aantal ontwerpprincipes (*privacy design patterns*) kan helpen bij het ontwerp van een privacyvriendelijk systeem[31]. De Wbp kan daarbij gebruikt worden als instrument om informatie-uitwisseling slim in te richten. Hetzelfde geldt voor algemene rechtsstatelijke beginselen, zoals de beginselen van subsidiariteit, proportionaliteit en specialiteit. Het meest bekend zijn de volgende principes.

Select before you collect. Dit principe staat ook wel bekend als het dataminimalisatie principe. Volgens dit principe mag je niet eerst alle mogelijke informatie verzamelen om vervolgens te kijken welke informatie je echt nodig hebt. In plaats daarvan moet je meteen beoordelen of je een bepaald data item nodig hebt, en mag je het alleen verzamelen en verder verwerken als dit inderdaad zo is[32]. Dit principe komt overeen met de eis van doelbinding binnen de Wbp en artikel 3 van de Wet Politiegegevens.

Context separation. Dit principe vereist – overeenkomstig bijvoorbeeld artikel 9 Wbp (verenigbaar gebruik) – dat gegevens over een persoon uit de ene context niet (zonder toestemming) gebruikt worden in een andere context, of gecombineerd worden met gegevens over deze persoon uit een andere context. Informatiestromen uit verschillende contexten

---

[30] Lessig, L. Code and other laws of cyberspace. Basic Books, 1999.

[31] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Privacy Enhancing Technologies. Witboek voor beslissers, december 2004.

[32] Jacobs, B. Select before you collect. Ars Aequi 54 (Dec. 2005), 1006–1009.

moeten dus gescheiden gehouden worden. Dit principe onderkent dat een persoon niet één vaste identiteit heeft, maar verschillende identiteiten kan hebben die in verschillende contexten naar voren komen. Mensen hebben verschillende rollen en verantwoordelijkheden in verschillende contexten en zullen zich daarom in de ene context anders gedragen dan in de andere context. Informatie over een persoon in de ene context is irrelevant of misschien zelfs schadelijk in een andere context. In geval van PET's betekent dit dat identiteits- en pseudo-identiteitsdomeinen binnen informatiesystemen gesplitst dienen te worden via een *identity-protector*.[33]

Anonimiseren. Dit principe gaat nog een stap verder en vereist dat alle gegevens die er voor zorgen dat de informatie tot een persoon herleidbaar is, wordt verwijderd. In feite zorgt het ervoor dat de informatie niet langer persoonlijke informatie is. Dit is lang niet zo eenvoudig als het op het eerste oog lijkt. Vaak is het zo dat een aantal, ieder op zich vrij algemene, kenmerken een persoon uniek kunnen identificeren.

Strikte toepassing van de deze *privacy design patterns* is niet altijd mogelijk of wenselijk. Zo is het principe van *select before you collect* incompatibel met het verdienmodel van vele gratis websites die hun omzet maken met het vergaren van zoveel mogelijk informatie over hun bezoekers. Ongelimiteerd informatie verzamelen leidt echter lang niet altijd tot efficiëntieverbetering. Verouderde of irrelevante informatie is eerder een last dan een lust[34]. *Context separation* moet er niet toe leiden dat burgers voor iedere overheidsdienst apart gevraagd moet worden om hun huidige adres. Strikte anonimisering kan data volstrekt onbruikbaar maken. Soms is het gewenst om gebruik te maken van pseudoniemen (bijvoorbeeld een betekenisloos nummer) om bepaalde partijen de mogelijkheid te geven om onder voorwaarden bestanden te koppelen. Hoe de *design patterns* moeten worden ingepast binnen het systeem is soms een afweging tussen privacy en functionaliteit. We zullen hierop in de volgende paragraaf verder ingaan.

4. Keuze: het proces

Naast het kiezen voor een *privacy by design* benadering als uitgangspunt voor het ontwerp en ontwikkeltraject van een systeem, bepaalt ook het doel van het systeem in grote mate de privacy-impact van het uiteindelijke systeem. Keuzes in functionaliteit hebben soms

---

[33] J. Borking, Der Identity-Protector, In Datenschutz und Datensichterheit (DuD) 1996, nr. 11.

[34] Verouderde, en dus foutieve informatie kan zeer schadelijk zijn, bijvoorbeeld in medische of financiële toepassingen. Het verzamelen van irrelevante informatie is niet conform de Wbp, en kan bij veiligheidsincidenten waarbij hackers toegang krijgen tot deze gegevens (zoals de laatste tijd weer veel in het nieuws is geweest) tot imagoschade en claims dan wel boetes leiden.

verstrekkende gevolgen wat betreft de complexiteit van de privacybeschermende maatregelen. We zullen dit verduidelijken aan de hand van twee voorbeelden: het EPD en het persoonlijk gezondheidsdossier. We proberen waar mogelijk de twee casus te toetsen aan de beschreven principes.

4.1. Het Elektronisch Patiënten Dossier

In de politieke discussie over het wetsvoorstel voor een landelijke EPD (L-EPD) was het redden van het leven van een zo groot mogelijk aantal patiënten, bijvoorbeeld door het voorkomen van verkeerd medicatiegebruik, een belangrijk doel.[35] Andere doelen van de stapsgewijs te realiseren landelijke infrastructuur voor de zorg waren kostenbesparing en kwaliteitsverbetering. De stuwende beginselen effectiviteit (in de vorm van kwaliteitsverbetering in de zorg) en efficiency (in de vorm van kostenbesparing) stonden centraal bij het wetgevingsproces.

Het efficiencydoel is van uit privacyperspectief geen onoverkomelijk probleem. Voor efficiëntieverhoging in de zorg is het voldoende om een standaard systeem van informatie uitwisseling op te zetten tussen zorgverleners onderling. Wel is het van belang dat bij ieder verzoek om informatie de patiënt – vanwege het medisch beroepsgeheim, zoals onder andere is bepaald in artikel 7: 457 BW – in beginsel toestemming voor deze uitwisseling wordt gevraagd. Het wetsvoorstel voor het L-EPD gaf de Staat als verantwoordelijke in de zin van de Wbp een wettelijke grondslag om de gegevens te mogen verwerken via een zogenaamde verwijsindex, zonder dat aan een ieder vooraf om uitdrukkelijke toestemming hoefde te worden gevraagd. Het wetsontwerp is op 5 april 2011 unaniem door de Eerste Kamer verworpen[36]. De inzet van PET's, vormen van *privacy by design* of juridische bescherming *by design* kwamen bij de voorbereiding van het wetsvoorstel en in het parlementaire debat echter nauwelijks aan de orde.[37]

Inmiddels is er een doorstartmodel [38] - voorlopig zonder bijbehorende wet – waarbij een nieuw opgerichte Vereniging van Zorgaanbieders de verantwoordelijke is en de patiënten om uitdrukkelijke toestemming gevraagd gaat worden. Het CBP ziet geen onoverkomelijke risico's

---

[35] Pluut B., Het landelijk EPD als black-box, WRR-webpublicatienummer 45, www.wrr.nl

[36] Zie Kamerstukken I 2011, 31 466.

[37] Zie voor een overzicht van zowel de juridische als de overige relevante argumenten tijdens het publiek debat over het EPD: Hooghiemstra T.F.M. en J. Nouwt, eHealth en Recht. Inleiding op het thema., Computerrecht, aflevering 6. December 2011, p.285-288.

[38] http://www.rijksoverheid.nl/onderwerpen/elektronisch-patientendossier/documenten-en-publicaties/notas/2012/01/19/vertrouwd-veilig-en-beheersbaar.html.

in dit plan[39], met name niet omdat het model uitgaat van toestemming van de patiënt voor gegevensverwerkingen conform de zienswijze van het CBP van 9 augustus 2011.[40]

Toestemming is niet in een systeem te vangen en daarmee geen voorbeeld van *privacy by design*. Wel is de wijze waarop toestemming wordt verkregen en vastgelegd een architectonisch vraagstuk. Met het verkrijgen van toestemming van de patiënt zijn echter niet alle en ook niet de belangrijkste rechtsstatelijke vraagstukken opgelost. Ook voor privacy is toestemming geen garantie, onder andere vanwege de mogelijkheid dat mensen ten gevolge van sociale, financiële druk of druk van politie en justitie toestemming verlenen. Bij het L-EPD kan het medisch beroepsgeheim van de zorgverleners – zoals andere is vastgelegd in artikel 7: 457 BW – die bescherming bieden. Ook het in de Wbp en andere wetgeving verankerde doelbinding- en proportionaliteitsbeginsel zijn naast toestemming minstens zo belangrijk voor de privacybescherming.

Een vervolgvraag bij het L-EPD is in hoeverre de verzamelde data gebruikt mogen worden voor statistisch beleids- en wetenschappelijk onderzoek. Voor het doen van statistisch onderzoek gebaseerd op gegevens uit het L-EPD is op grond van de Wbp en de Wet geneeskundige behandelingsovereenkomst (Wgbo, boek 7 BW) anonimisering vereist. Hildebrandt laat in haar oratie zien dat ook geanonimiseerde gegevens gebruikt kunnen worden om profielen van mensen of groepen aan te maken op basis waarvan keuzes gemaakt kunnen worden die van invloed zijn op iemands leven.[41] Wij stellen ons de vraag: is voor echte keuzevrijheid en zelfbeschikking van de patiënt een intelligente *software agent* (soft- en hardware die in staat is autonoom te handelen om een taak uit te voeren voor haar gebruiker) een mogelijke oplossingsrichting? Zo'n *agent* is grof gezegd een stuk software dat zelfstandig de belangen van zijn eigenaar behartigt. Weliswaar kunnen en mogen we de bescherming van privacy als publiek goed niet alleen op de schouders van individuele burgers leggen en hen daar zeker niet toe verplichten, maar een deel van de oplossing zou hier kunnen liggen. In het Privacy Incorporated Software Agent (*PISA)-project* is aangetoond dat *intelligent software agents* beslissingen kunnen nemen om de privacy van personen te beschermen, mits de juiste juridische kennis in de vorm van beslissingsregels wordt ingebouwd.[42]

---

[39] http://www.rijksoverheid.nl/onderwerpen/elektronisch-patientendossier/documenten-en-publicaties/brieven/2012/01/19/brief-over-de-doortstart-van-een-landelijke-infrastructuur-uitwisseling-medische-gegevens.html

[40] Zie zienswijze Doorstartmodel EPD van het CBP, www.cbpweb.nl

[41] M. Hildebrandt, De rechtsstaat in cyberspace, Nijmegen: uitgegeven in eigen beheer 2011

[42] Zie Borking, J. Privacyrecht is code, 2010 p.233-235 en 282 -291

4.2. Het Persoonlijk gezondheidsdossier

In aanvulling op het EPD is de opkomst van persoonlijke gezondheidsdossiers (PGD's) actueel. Het doel van het PGD is dat het een dossier is waarmee de patiënt zelf begint en dat hij zelf bijhoudt. Het gezondheidsdossier is geen volledig medisch dossier. Het is vooral een werkomgeving voor de patiënt, waarin de eigen medische gegevens bijgehouden kunnen worden en gegevens van anderen, zoals zorgverleners, te down- of te uploaden zijn. De patiënt kan de zorgverleners eventueel ook toegang geven. Het gebruik van PGD's wordt steeds meer gestimuleerd vanuit de overheid, de zorgaanbieders en de ICT-markt. Wat betreft zelfbeschikking en keuzevrijheid is naast het doorstart model voor het L-EPD van belang dat de Nederlandse Patiënten en Consumentenfederatie (NPCF) van VWS onlangs financiële middelen heeft gekregen om op landelijke schaal een Persoonlijk Gezondheidsdossier (PGD) te faciliteren. Sommige zorgaanbieders en patiëntenorganisaties ontwikkelen al PGD's, zoals Zorgnet in Nijmegen en de PGD van de Diabetes Vereniging Nederland. In de markt zijn PGD's als Medlook en HealthVault van Microsoft in opkomst.

Juridisch gezien is het PGD vanwege de dossierplicht van de zorgverlener (artikel 7:454, eerste lid, BW) in het geldende recht geen alternatief voor de medische gegevens die de hulpverlener[43] dient bij te houden. De Wgbo maakt het voor de patiënt mogelijk om van het aanvullingsrecht gebruik te maken. Het zou ideaal zijn als beide dossiers elkaar aanvullen en onderling patiëntgegevens uitwisselen, mits deze uitwisseling van zodanige soft-, hardware en architectuur gebruikt maakt dat de privacy, keuzevrijheid en andere rechten van de patiënt voldoende beschermd worden. Bijvoorbeeld door pseudo-identiteiten en identiteitsdomeinen te gebruiken, zodat gegevens niet los van de persoon gaan 'zwerven'.

Er is nog juridische en technologische arbeid nodig. Zo wordt het PGD niet beschermd door het medisch beroepsgeheim. Medische gegevens in het PGD kunnen onder sociale of financiële druk ook inzichtelijk worden voor personen en instanties buiten de gezondheidszorg. Ook kan in een rechtszaak de patiënt tot gegevensverstrekking uit het PGD worden gedwongen waar de arts zich op het verschoningsrecht zou kunnen beroepen. Het is de moeite waard om te onderzoeken of er zoiets als een patiëntengeheim moet komen voor het PGD. Weliswaar is zijn de artikelen 6 (zoals doelbinding) en 8 (uitdrukkelijke toestemming) van de Richtlijn 95/46/EG en minimaal de artikelen 8 jo. 21 Wbp van toepassing, maar toestemming is geen afdoende garantie voor privacy.

In het kader van goede code is de kernvraag: in hoeverre kan technologie behulpzaam zijn om de patiënt echt zeggenschap te geven over zijn dossier? Gedacht kan worden aan versleutelde opslag van de gegevens die alleen met actieve tussenkomst van de gebruiker kunnen worden uitgewisseld. Directe toegang door derden kan beperkt worden tot een gelimiteerde verzameling gegevens. Eventueel kan ook een derde partij voorzien worden van een

[43] In de zin van de Wgbo.

noodtoegangssleutel. Van de wetgever zou gevraagd kunnen worden om technologie waarmee de zeggenschap van de patiënt redelijkerwijs gerealiseerd kan worden voor te schrijven.

5. Conclusies

Het doel van een ICT systeem bepaalt de functionaliteit en de functionaliteit bepaalt de uiteindelijke architectuur van het systeem. Dit doel wordt door de (politieke of ambtelijke) opdrachtgever bepaald. Hierbij moet de wetgever zich ervan bewust zijn dat, net als bij geschreven regelgeving, allerlei neveneffecten kunnen optreden die het oorspronkelijke doel kunnen overstemmen. Privacy en keuzevrijheid zijn voorbeelden van eigenschappen van het systeem die afhankelijk zijn van de architectuur. Bij het invoeren van een landelijk ICT systeem is het daarom belangrijk om transparant te zijn over de doelen, de daaruit voortvloeiende architectuur, en goed te kijken naar de consequenties van deze keuzes. Het principe van 'code is law' kan helpen om de (negatieve) impact van het ICT-systeem op de grondrechten te beperken.

Terecht vindt het 'law is code' kamp dat vanuit het perspectief van de democratische rechtsstaat het wenselijk is dat ICT ondergeschikt is aan wet- en regelgeving. Met andere woorden: de keuze voor een bepaalde opzet van een systeem is in hoge mate ook een politieke dan wel beleidsmatige keuze.

Het is daarom essentieel om te komen tot 'goede code', oftewel code waarvan het normen en waardenstelsel ("code is law") het resultaat is van een democratisch beslissingsproces ("law is code"). Dit als fundamentele bescherming van onze grondrechten in de steeds verder digitaliserende maatschappij.

Goede code is het resultaat van een aantal vaste stappen bij het ontwikkelen van een systeem. In het geval van een landelijk ICT systeem zal dit systeem geflankeerd worden door wetgeving over het gebruik van het systeem (zoals het geval is geweest bij het Elektronisch Patiënten Dossier en ook voor de invoering van de slimme energiemeter[44]). Eerst zal de politiek een uitspraak moeten doen over het doel en de reikwijdte van het desbetreffende systeem door middel van wetgeving. Het ontwerp van de wetgeving dient hand in hand te gaan met het ontwerp van een passende architectuur voor het systeem. Deze twee fasen lopen parallel en idealiter geïntegreerd, waarbij een optimale balans tussen juridische en technische verankering wordt gezocht. Juridische bescherming *by design* moet een serieuze optie worden bij het articuleren van rechtsnormen. We moeten goed kijken hoe de *defaults* van de ICT

[44] Op 9 november 2011 stemde de Tweede Kamer in met de Novelle wijziging wetsvoorstel verbetering marktmodel (TK 32 374) en de Novelle wijziging wetsvoorstel implementatie energie efficiëntie (TK 32 373).

infrastructuur zich ontwikkelen en bijsturen of ingrijpen als die het uitoefenen van grondrechten verhinderen. Dat vereist nieuwe vormen van samenwerking tussen juristen en computerwetenschappers en reflectie op de verhouding tussen recht en bijvoorbeeld machinaal lerende beslissystemen. We zullen moeten ontdekken hoe juridische bescherming op het meest geëigende niveau in te bouwen is in de hard- en software.